PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-025045
(43)Date of publication of application : 29.01.1999

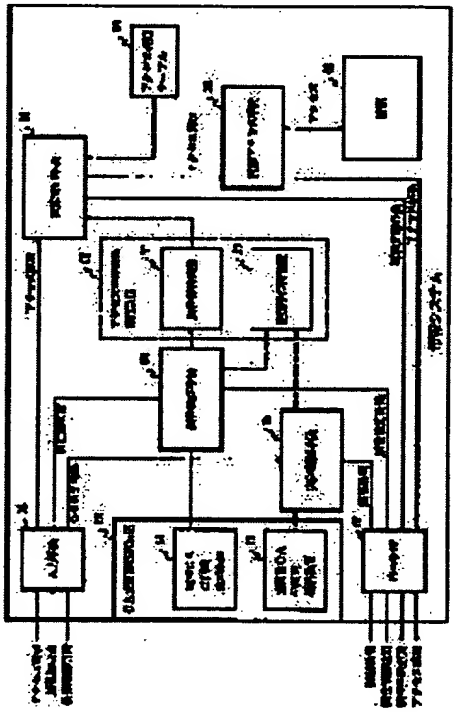
(51)Int.Cl. G06F 15/00
G06F 12/14
H04L 9/32

(21)Application number : 09-189041
(22)Date of filing : 30.06.1997

(71)Applicant : NEC CORP
(72)Inventor : YAMAOKA YOSHIJI

(54) ACCESS CONTROL METHOD, ITS DEVICE, ATTRIBUTE CERTIFICATE ISSUING DEVICE, AND MACHINE-READABLE RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an access control method capable of simply setting up an access rule even when an access subject is not known, of checking whether the access subject has authority or not and of easily executing user management.
SOLUTION: Data which provide partial information of an access subject or which describe characteristics of the access subject are defined as an attribute. Attributes required for accessing each of all resources 01 in an information system are set up in an access rule table 08. A substance certification means 02 certificates a substance of the access subject, an attribute verification means 03 determines whether the attribute of the access subject exists or not, and a resource management means 04 determines whether an access request from the access subject to the resources 01 is allowed or not. An attribute certificate presented by the access subject is used for the judgement of existence of the attribute.



LEGAL STATUS

[Date of request for examination] 30.06.1997
[Date of sending the examiner's decision of rejection] 10.07.2001
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－25045

(43)公開日　平成11年(1999)１月29日

(51)Int.Cl.[6]		識別記号	FI		
G06F	15/00	330	G06F	15/00	330A
	12/14	310		12/14	310K
H04L	9/32		H04L	9/00	675B

審査請求　有　　請求項の数27　FD　（全 23 頁）

(21)出願番号　特願平9－189041

(22)出願日　平成９年(1997)６月30日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　山岡　誉侍
東京都港区芝五丁目７番１号　日本電気株式会社内

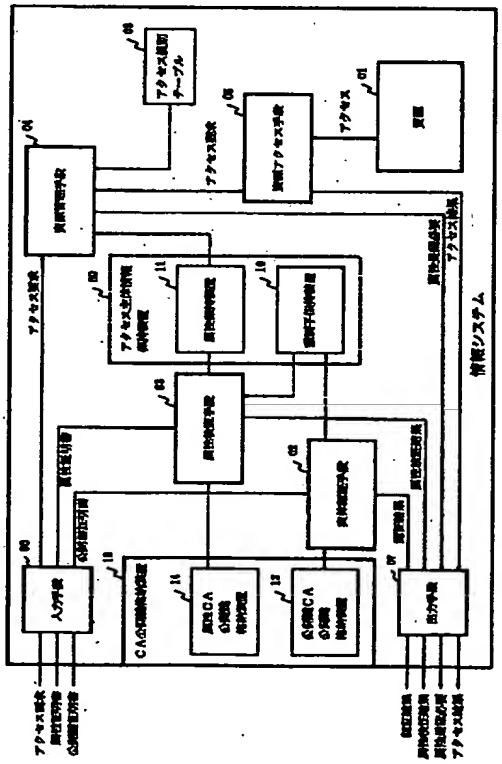
(74)代理人　弁理士　境　廣巳

(54)【発明の名称】　アクセス制御方法とその装置及び属性証明書発行装置並びに機械読み取り可能な記録媒体

(57)【要約】

【課題】　アクセス主体を知らなくてもアクセス規則の設定を単純に行うことができ、しかも、アクセス主体が権限を持つことの確認も可能で、さらに、ユーザ管理の容易なアクセス制御の方法を提供する。

【解決手段】　アクセス主体の一部の情報を与える、或いはアクセス主体の特性を記述するデータを、属性と定義する。アクセス規則テーブル08は、情報システム内に全ての資源01毎にそのアクセスに必要な属性を設定してある。実体認証手段02でアクセス主体の実体認証を行い、属性検証手段03でアクセス主体の属性の認否の判定を行い、資源管理手段04で資源01に対するアクセス主体からのアクセス要求の可否を判定する。属性の認否の判定には、アクセス主体が提示する属性証明書を用いる。



【特許請求の範囲】

【請求項1】 情報システムの資源に対するアクセス主体からのアクセスをアクセス規則に基づき制御する方法において、アクセス主体の属性によりアクセス規則を設定し、アクセス主体の属性を是認することで制御を行うことを特徴とするアクセス制御方法。

【請求項2】 情報システムの資源に対するアクセス主体からのアクセスをアクセス規則に基づき制御する方法において、アクセス主体の属性によりアクセス規則を設定し、アクセス主体の実体認証を行い、アクセス主体の属性を是認することで制御を行うことを特徴とするアクセス制御方法。

【請求項3】 アクセス主体の属性、および、属性による条件式、属性の演算式、属性の論理式により、アクセス規則を設定することを特徴とする請求項1または2記載のアクセス制御方法。

【請求項4】 アクセス主体の属性の是認を属性情報テーブルを用いることにより行うことを特徴とする請求項1、2または3記載のアクセス制御方法。

【請求項5】 アクセス主体の属性の是認をアクセス主体が提示してきた属性情報に対して行うことを特徴とする請求項1、2または3記載のアクセス制御方法。

【請求項6】 アクセス主体の属性の提示をデジタル署名を施された属性証明書を用いることにより行うことを特徴とする請求項5記載のアクセス制御方法。

【請求項7】 アクセス主体の属性の提示を公開鍵証明書を用いることにより行うことを特徴とする請求項5記載のアクセス制御方法。

【請求項8】 アクセス主体の実体認証をパスワードにより行うことを特徴とする請求項2、3、4、5または6記載のアクセス制御方法。

【請求項9】 アクセス主体の実体認証を公開鍵証明書を用いることにより行うことを特徴とする請求項2、3、4、5、6または7記載のアクセス制御方法。

【請求項10】 アクセス主体の実体認証をデジタル署名を施された属性証明書を用いることにより行うことを特徴とする請求項2、3、5または6記載のアクセス制御方法。

【請求項11】 情報システムの資源に対するアクセス主体からのアクセスをアクセス規則に基づき制御する装置において、アクセス主体の属性によりアクセス規則を設定するテーブルを備えることを特徴とするアクセス制御装置。

【請求項12】 情報システムの資源に対するアクセス主体からのアクセスをアクセス規則に基づき制御する装置において、アクセス主体の属性によりアクセス規則を設定するテーブルと、アクセス主体の属性を是認する手段とを備えることを特徴とするアクセス制御装置。

【請求項13】 情報システムの資源に対するアクセス主体からのアクセスをアクセス規則に基づき制御する装置において、アクセス主体の属性によりアクセス規則を設定するテーブルと、アクセス主体の属性を是認する手段と、アクセス主体の実体認証を行う手段とを備えることを特徴とするアクセス制御装置。

【請求項14】 アクセス主体の属性、および、属性による条件式、属性の演算式、属性の論理式により、アクセス規則を設定するテーブルを備えることを特徴とする請求項11、12または13記載のアクセス制御装置。

【請求項15】 属性情報を保存したテーブルを参照し属性是認する手段を備えることを特徴とする請求項12、13または14記載のアクセス制御装置。

【請求項16】 属性情報を記載した属性証明書を検証して属性是認する手段を備えることを特徴とする請求項12、13または14記載のアクセス制御装置。

【請求項17】 属性情報を記載した公開鍵証明書で認証して属性是認する手段を備えることを特徴とする請求項12、13または14記載のアクセス制御装置。

【請求項18】 パスワードにより実体認証する手段を備えることを特徴とする請求項13、14、15または16記載のアクセス制御装置。

【請求項19】 公開鍵証明書を用いることにより実体認証する手段を備えることを特徴とする請求項13、14、15、16または17記載のアクセス制御装置。

【請求項20】 属性証明書を用いることにより実体認証する手段を備えることを特徴とする請求項13、14または16記載のアクセス制御装置。

【請求項21】 アクセス主体の属性から属性証明書本文を作成する手段と、属性証明書本文にデジタル署名を行い属性証明書署名文を作成する手段と、属性証明書本文と属性証明書署名文から属性証明書を作成する手段とを備えることを特徴とする属性証明書発行装置。

【請求項22】 アクセス主体の属性と識別子から属性証明書本文を作成する手段と、属性証明書本文にデジタル署名を行い属性証明書署名文を作成する手段と、属性証明書本文と属性証明書署名文から属性証明書を作成する手段とを備えることを特徴とする属性証明書発行装置。

【請求項23】 アクセス主体の属性と公開鍵から属性証明書本文を作成する手段と、属性証明書本文にデジタル署名を行い属性証明書署名文を作成する手段と、属性証明書本文と属性証明書署名文から属性証明書を作成する手段とを備えることを特徴とする属性証明書発行装置。

【請求項24】 情報システムの資源に対するアクセス主体からのアクセスを、アクセス主体の属性により記述されたアクセス規則に基づき制御するプログラムであって、コンピュータに、パスワード照合によりアクセス主体の実体認証を行うステップと、アクセス主体の実体認証が成功するまでアクセス主体からの資源に対するアクセスを制限するステップと、アクセス主体の実体認証の

成功後に、アクセス主体が資源にアクセスするために必要な属性を保有しているか否かを、各アクセス主体の属性を設定してある属性情報テーブルおよび前記アクセス規則を設定してあるアクセス規則テーブルを参照して判断するステップと、アクセス主体の属性が是認されるまでアクセス主体からの資源に対するアクセスを制限するステップとを行わせるプログラムを記録した機械読み取り可能な記録媒体。

【請求項25】 情報システムの資源に対するアクセス主体からのアクセスを、アクセス主体の属性により記述されたアクセス規則に基づき制御するプログラムであって、コンピュータに、アクセス主体が提示する公開鍵証明書によりアクセス主体の実体認証を行うステップと、アクセス主体の実体認証が成功するまでアクセス主体からの資源に対するアクセスを制限するステップと、アクセス主体の実体認証の成功後に、アクセス主体が資源にアクセスするために必要な属性を保有しているか否かを、各アクセス主体の属性を設定してある属性情報テーブルおよび前記アクセス規則を設定してあるアクセス規則テーブルを参照して判断するステップと、アクセス主体の属性が是認されるまでアクセス主体からの資源に対するアクセスを制限するステップとを行わせるプログラムを記録した機械読み取り可能な記録媒体。

【請求項26】 情報システムの資源に対するアクセス主体からのアクセスを、アクセス主体の属性により記述されたアクセス規則に基づき制御するプログラムであって、コンピュータに、アクセス主体が提示する公開鍵証明書によりアクセス主体の実体認証を行うステップと、アクセス主体の実体認証が成功するまでアクセス主体からの資源に対するアクセスを制限するステップと、アクセス主体の実体認証の成功後に、アクセス主体が提示する属性証明書によりアクセス主体の属性を是認するステップと、アクセス主体の属性が是認されるまでアクセス主体からの資源に対するアクセスを制限するステップと、是認したアクセス主体の属性と前記アクセス規則を設定してあるアクセス規則テーブルとに基づいて資源に対するアクセス主体からのアクセスの可否を判断するステップとを行わせるプログラムを記録した機械読み取り可能な記録媒体。

【請求項27】 情報システムの資源に対するアクセス主体からのアクセスを、アクセス主体の属性により記述されたアクセス規則に基づき制御するプログラムであって、コンピュータに、アクセス主体が提示する、アクセス主体の公開鍵及び属性を証明する証明書によりアクセス主体の実体認証を行うステップと、アクセス主体の実体認証が成功するまでアクセス主体からの資源に対するアクセスを制限するステップと、アクセス主体の実体認証の成功後に、前記証明書によりアクセス主体の属性を是認するステップと、アクセス主体の属性が是認されるまでアクセス主体からの資源に対するアクセスを制限するステップと、是認したアクセス主体の属性と前記アクセス規則を設定してあるアクセス規則テーブルとに基づいて資源に対するアクセス主体からのアクセスの可否を判断するステップとを行わせるプログラムを記録した機械読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報システム内の資源に対するユーザなどのアクセスを制御する方法および装置に関する。

【0002】

【従来の技術】従来、情報システムのアクセス制御は、資格のないアクセス主体の接近から、内部の資源を守るために、アクセス規則を設定して、その規則に応じて、資源へのアクセスを制限することにより、資源の保護を行ってきた。ここで、アクセス主体とは、ユーザ、プロセス、機器、などのことを表し、また、資源とは、データ、ファイル、プログラム、アプリケーション、サービス、機器、などのことを表す。「暗号とデータセキュリティ」（D.E.R.デニング著、1988年発行、培風館）の4章や、「情報システムのセキュリティ」（上園忠広著、1995年発行、トッパン）のP.143～155には、アクセス制御について、詳しく述べられている。

【0003】アクセス規則の設定には、アクセス権限行列、あるいは、許可リスト、資格リストなどのテーブルが用いられる。アクセス権限行列とは、アクセス主体の資源に対する権限が定義された行列である。権限とは、読み出し可能、書き込み可能、更新可能、削除可能、実行可能、などの機能のことである。許可リストは、特定の資源に対して設定されたリストであり、アクセス主体の権限を定義する。資格リストは、特定のアクセス主体に対して設定されたリストであり、資源に対する権限を定義する。

【0004】情報システムでアクセス規則を設定するためには、情報システムでアクセス主体を識別することが必要になり、各アクセス主体に対して識別子を用意することで、その識別子を用いてアクセス規則の設定を行っている。

【0005】アクセス規則の設定を簡易に行うための方法としては、アクセス主体を何らかの基準に応じてグループ化して、そのグループに対してアクセス規則を設定する方法がある。

【0006】しかし、例えば、アクセス主体がユーザのとき、識別子を用意するだけでは、ユーザが本当に当人であるということを保証できない。そのため、ユーザが正当であることを確認する実体認証の技術も重要になる。実体認証の方法としては、パスワードの入力がよく用いられている。この方法では、識別子・パスワードの対になったパスワード情報を参照することにより、実体認証を行う。

【０００７】ユーザに識別子を用意すること、および、パスワード情報を設定することは、一般にユーザ登録と呼ばれている。

【０００８】結局、従来の情報システムでアクセス制御を行うためには、ユーザ登録により、ユーザ識別、ユーザ認証を行うことが前提になる。

【０００９】また、実体認証の方法としては、非対称暗号系を用いる方法がある。非対称暗号系とは、一般に公開された公開鍵と本人のみが秘密に持つ秘密鍵により、暗号化・復号を行う技術である。実体認証に用いる場合は、秘密鍵の所持により本人であることを主張する。非対称暗号系を実体認証に用いる方法については、米国特許の4,405,829,「CRYPTOGRAPHIC COMMUNICATIONS SYSTEM AND METHOD」や、ＩＳＯ／ＩＥＣ9793-3「Information technology-Security techniques-Entity authentication mechanisms-Part3: Entity authentication using a public keyalgorithm」に詳しく述べられている。

【００１０】デジタル署名は、文書の作成者が本人であること、文書の正当性・完全性、を確認する技術であり、主に非対称暗号系を利用する。この場合、秘密鍵で署名文の作成を行い、公開鍵で署名の確認を行う。「E-Mailセキュリティ」（Bruce Schneier 著、１９９５年、オーム社）の第4章では、デジタル署名について詳しく述べられている。

【００１１】非対称暗号系では、公開鍵が偽造されたものでないことの証明のために、信頼できる第三者によるデジタル署名をつけた公開鍵証明書を発行する。証明書を発行する機関はＣＡと呼ばれる。上記「E-Mailセキュリティ」の第5章では、公開鍵証明書、ＣＡについて詳しく述べられている。ここでは、特にＣＡを公開鍵ＣＡと呼ぶことにする。

【００１２】

【発明が解決しようとする課題】従来の技術では、情報システムで、ある資格を持ったユーザに何らかのサービスを提供する場合、ユーザ単位にアクセス規則を設定し、アクセスを制御する。しかし、この方法では、第1の問題として、ユーザを識別、実体認証できなければならないので、情報システムごとに事前のユーザ登録が必要になる点が挙げられる。また、第2の問題として、アクセス規則の設定は、登録ユーザごとに行わなくてはならない点が挙げられる。さらに、第3の問題として、アクセス主体自身とアクセス主体が権限を持つ資格があるかどうかを知っていなければ、アクセス規則の設定ができない点が挙げられる。

【００１３】また、アクセス規則の設定を簡易に行うため、ユーザをあらかじめグループ化し、グループ単位でアクセス規則を設定する方法がある。しかし、この方法では、第4の問題として、ユーザは複数の情報システムを利用する場合にはそれぞれの情報システムごとの登録が必要になるので、ユーザの情報に変更が生じ、グループ化の基準も変わった場合には、全ての情報システムにおいて、グループ情報の変更が必要になるという点が挙げられる。

【００１４】そこで、ユーザ登録情報とグループ情報を少数のサーバで一括に管理し、情報システムは、ユーザ認証を行う場合やグループ情報を確認する場合には、サーバに問い合わせを行う方法が考えられる。しかし、この方法では、第5の問題として、サービスを提供する情報システムの方では、自由にユーザのグループ化を行うことができないという点が挙げられる。

【００１５】本発明の目的は、アクセス主体を知らなくてもアクセス規則の設定を単純に行うことができて、しかも、アクセス主体が権限を持つことの確認も可能で、さらに、ユーザ管理の容易なアクセス制御の方法を提供することである。

【００１６】

【課題を解決するための手段】本発明では、アクセス主体の一部の情報を与える、あるいは、アクセス主体の特性を記述するデータを属性と定義する。属性は、属性型と属性値から構成される。これは、ＪＩＳ　Ｘ　5752-1993「開放型システム間相互接続ーディレクトリー第2部　モデル」8ページで述べられている定義である。

【００１７】属性型とは、属性によって与えられる情報の項目である。例えばアクセス主体がユーザの場合、氏名（姓、名）、性別、生年月日、住所、電話番号、電子メールアドレス、組織名、会社名、部署名、役職名、免許、資格、公開鍵、などが考えられる。

【００１８】属性値とは、属性型の実現値である。属性値の例としては、属性型「姓」に対して「山岡」、属性型「名」に対して「誉侍」、属性型「会社名」に対して「日本株式会社」、などである。

【００１９】属性の実際の表現方法としては、「姓：山岡」、「名：誉侍」、「会社名：日本株式会社」、などと表される。

【００２０】さらに、アクセス主体の属性に、その属性を証明する機関を用意する。この機関を属性ＣＡと呼ぶことにする。属性ＣＡは、アクセス主体の属性を証明する属性証明書の発行を行う。属性証明書は、アクセス主体の、単数あるいは複数の属性型に対する属性値が正当であることを証明するために、属性ＣＡのデジタル署名をつけた証明書である（第3、第4の実施の形態）。

【００２１】情報システムは、アクセス規則を、アクセス主体の属性、および、属性の条件式、属性の演算式、属性の論理式、などにより設定する。

【００２２】アクセス主体の属性については、あるテーブルに保存し、そのテーブルを参照する方法（第1、第2の実施の形態）、あるいは、アクセス主体の側で情報システムに提示してくる方法を用いる。アクセス主体の側で情報システムに提示してくる方法としては、属性証明書（第3、第4の実施の形態）、または、公開鍵証明

書(第4 の実施の形態) を用いる。

【００２３】アクセス主体の実体認証にはパスワード(第1 の実施の形態) 、あるいは、公開鍵証明書の提示(第2 ～第4 の実施の形態) 、属性証明書の提示(第4 の実施の形態) 、により行う。よって、アクセス主体の登録は、情報システムやネットワークで接続されたサーバ上で一括して行う 方法(第1 の実施の形態) 、あるいは、公開鍵ＣＡが担当する方法(第2 ～第4 の実施の形態) 、属性ＣＡが担当する方法(第4 の実施の形態) 、を用いる。

【００２４】

【 発明の実施の形態】図1 は本発明の第1 の実施の形態を示す情報システムのブロック図である。第1 の実施の形態では、パスワードを用いることによりアクセス主体の実体認証を行い、テーブルに保存された属性を参照することでアクセス主体の属性を確認して、アクセス規則に基づき資源に対するアクセスを制御する。

【００２５】以下、図1 を参照して、第1 の実施の形態を、情報システムの構成、各構成要素の機能、情報システムの動作の順で説明する。

【００２６】まず、図1 を参照して、情報システムの構成を説明する。

【００２７】情報システムは、資源０１を備え、アクセス主体からのアクセス要求などを管理する。また、情報システムは、資源０１の他に、アクセス要求の管理のために、実体認証手段８０２と、資源管理手段８０４と、資源アクセス手段０５と、入力手段０６と、出力手段０７と、アクセス規則テーブル０８と、アクセス主体情報保持装置０９とを有する。

【００２８】さらに、アクセス主体情報保持装置０９には、識別子保持装置１０と属性保持装置１１とが備えられる。

【００２９】また他に、パスワード情報格納装置８１３と属性情報テーブル８１４も用いるが、これらについては情報システム内の装置として構成してもよいし、ネットワークで接続された外部に存在してもよい。外部に設ける場合、複数の情報システムに共通なサーバ上に設けることが考えられる。

【００３０】以下、図1 を参照して、情報システムの各構成要素の機能を説明する。

【００３１】実体認証手段８０２は、アクセス主体の実体認証を行うための手段である。入力手段０６からの識別子・パスワードの受信とそれによる起動、パスワード情報格納装置８１３の参照、アクセス主体の識別子・パスワードによる実体認証、識別子保持装置１０への認証済アクセス主体の識別子の出力、出力手段０７への認証結果の送信と起動の指令、を行う。

【００３２】資源管理手段８０４は、資源０１に対するアクセス要求の認否を判定する手段である。入力手段０６からのアクセス要求の受信とそれによる起動、アクセス規則テーブル０８と属性保持装置１１の参照、識別子保持装置１０と属性情報テーブル８１４の参照、アクセス主体の属性の認否の判定、属性によるアクセス要求の認否の判定、属性保持装置１１へのアクセス主体の是認済属性の出力、出力手段０７へのアクセス不許可の送信と起動の指令、資源アクセス手段０５へのアクセス要求の送信と起動の指令、を行う。

【００３３】資源アクセス手段０５は、資源０１にアクセスできる手段である。資源管理手段８０４からのアクセス要求の受信とそれによる起動、アクセス要求の実行、出力手段０７への実行結果の送信と起動の指令、を行う。

【００３４】入力手段０６は、アクセス主体と情報システムとの対話を行う手段である。アクセス主体からのアクセス要求などの入力の受信、情報システム内の他の手段への情報の送信と起動の指令、を行う。

【００３５】出力手段０７は、アクセス主体と情報システムとの対話を行う手段である。情報システム内の他の手段からの情報の受信とそれによる起動、アクセス主体に対する処理結果などの出力、を行う。

【００３６】アクセス規則テーブル０８は、資源管理手段８０４がアクセス権限の検査を行うために用いるテーブルであり、情報システム内の全ての資源に対して、その資源にアクセス可能な属性が設定してある。図2 はアクセス規則テーブル０８の設定の例である。この例では、それぞれ、日本株式会社のX 部の部長にファイルＡの書き込み、高等学校教諭専修免許を持つアクセス主体にデータベースＢの読み出し、２０才以上にサービスＣの実行、の権限を与えている。この例のように、アクセス規則は、アクセス主体の属性、および、属性による条件式、属性の演算式、属性の論理式により設定することができる。

【００３７】アクセス主体情報保持装置０９は、アクセス主体の情報を保持する装置である。識別子保持装置１０は、実体認証手段８０２で実体認証されたアクセス主体の識別子(例えば、登録ユーザＩＤ) を保持する装置である。属性保持装置１１は、資源管理手段８０４で是認済のアクセス主体の属性を保持する装置である。

【００３８】パスワード情報格納装置８１３は、実体認証手段８０２でアクセス主体の実体認証に用いるための識別子とパスワードに関する情報を格納する装置である。

【００３９】属性情報テーブル８１４は、アクセス主体の識別子単位に属性を格納しているテーブルである。

【００４０】以下、図1 を参照して、情報システムの動作を説明する。

【００４１】アクセス主体が情報システムに送信できるのは、実体認証要求とアクセス要求の二つである。

【００４２】まず最初に、実体認証要求の処理を順に説明する。

【００４３】アクセス主体は、識別子・パスワードを入力手段０６に入力する。この入力された識別子・パスワードは入力手段０６から実体認証手段８０２に送信されて、認証の成否の判定に用いられる。

【００４４】識別子・パスワードを入力手段０６から受信した実体認証手段８０２は、パスワード情報格納装置８１３からパスワード情報を読み出し、識別子・パスワードを照合し、アクセス主体の認証を行う。認証が成功した場合は、アクセス主体の識別子を識別子保持装置１０に出力する。認証が失敗した場合は、識別子保持装置１０へのアクセス主体の識別子の出力は行わない。また、実体認証手段８０２は、出力手段０７に認証結果を送信して、起動を指令する。出力手段０７は認証の正否の結果をアクセス主体に出力する。

【００４５】次に、アクセス要求の処理を順に説明する。

【００４６】アクセス要求は、アクセス主体が認証済のときに行う。アクセス主体は、資源０１へのアクセス要求を入力手段０６に入力する。この入力されたアクセス要求は資源管理手段８０４に送信される。

【００４７】図3は資源管理手段８０４の動作の一例を示すフローチャートである。アクセス要求を入力手段０６から受信した（９０１）資源管理手段８０４は、アクセス規則テーブル０８を参照して、資源０１のアクセスに必要な属性を抽出する（９０２）。例えば資源０１が図2のデータベースBの場合、「免許：高等学校教諭専修」なる属性を抽出する。次に、属性保持装置１１を参照してアクセスに必要な属性が是認済かを確認する（９０３）。属性が是認済であれば、資源０１へのアクセスを認可して（９０４）、資源アクセス手段０５にアクセス要求を送信して、起動を指令する（９０５）。資源アクセス手段０５は、アクセス要求を資源０１に対して実行し、その結果は出力手段０７に送信されてアクセス主体に出力される。

【００４８】属性が是認済でなければ、資源管理手段８０４は、識別子保持装置１０を参照して、アクセス主体が認証済であるかを確認する（９０６）。認証済でなければ、出力手段０７に認証要求の処理が必要であることを送信して、起動を指令する（９０７）。認証済であれば、識別子保持装置１０からアクセス主体の識別子を読み出し（９０８）、属性情報テーブル８１４を参照して（９０９）、資源０１のアクセスに必要な属性をアクセス主体が持っているかを検証する（９１０）。アクセス主体が該当する属性を持っていない場合は、資源０１へのアクセスを不許可にして、出力手段０７にアクセス不許可を送信して、起動を指令する（９１１）。アクセス主体が該当する属性を持っている場合は、その属性を是認して（９１２）、アクセス主体の属性を属性値保持装置１１に出力して（９１３）、さらに、資源０１へのアクセスを認可して（９０４）、資源アクセス手段０５にアクセス要求を送信して、起動を指令する（９０５）。

【００４９】上述のように構成された本発明の第1の実施の形態によれば、アクセス主体の属性によりアクセス規則の設定を行うため、アクセス規則の設定が単純に行える。それにより、資源のアクセス規則の設定者（例えばサービスの提供者）は、アクセス主体を知らない場合でもアクセスを許可することが可能となる。

【００５０】図4は本発明の第2の実施の形態を示す情報システムのブロック図である。第2の実施の形態では、公開鍵証明書を用いることによりアクセス主体の実体認証を行い、テーブルに保存された属性を参照することでアクセス主体の属性を確認して、アクセス規則に基づき資源に対するアクセスを制御する。

【００５１】以下、図4を参照して、第2の実施の形態を、情報システムの構成、各構成要素の機能、情報システムの動作の順で説明する。

【００５２】まず、図4を参照して、情報システムの構成を説明する。

【００５３】情報システムは、資源０１を備え、アクセス主体からのアクセス要求などを管理する。また、情報システムは、資源０１の他に、アクセス要求の管理のために、実体認証手段０２と、資源管理手段８０４と、資源アクセス手段０５と、入力手段０６と、出力手段０７と、アクセス規則テーブル０８と、アクセス主体情報保持装置０９とを有する。

【００５４】さらに、アクセス主体情報保持装置０９には、識別子保持装置１０と属性保持装置１１とが備えられる。

【００５５】また他に、ＣＡ公開鍵格納装置１２と属性情報テーブル８１４も用いるが、これらについては情報システム内の装置として構成してもよいし、ネットワークで接続された外部に存在してもよい。

【００５６】さらに、ＣＡ公開鍵格納装置１２には、公開鍵ＣＡ公開鍵格納装置１３が備えられる。

【００５７】以下、図4を参照して、情報システムの各構成要素の機能を説明する。

【００５８】実体認証手段０２は、アクセス主体の実体認証を行うための手段である。第1の実施の形態の実体認証手段８０２とは異なり、認証を行うために公開鍵証明書を用いる。公開鍵証明書には、例えば図5に示すように、アクセス主体の公開鍵、アクセス主体の識別子（例えば電子メールアドレス）、氏名、証明書を発行してＣＡのデジタル署名が記載される。実体認証手段０２は、入力手段０６からの公開鍵証明書と認証情報の受信とそれによる起動、公開鍵ＣＡ公開鍵格納装置１３からの公開鍵の読み出し、公開鍵証明書の公開鍵ＣＡの署名の検証、アクセス主体の非対称暗号系における認証方法による実体認証、および、識別子保持装置１０への認証済アクセス主体の公開鍵証明書に記載の識別子の出力、出力手段０７への認証結果の送信と起動の指令、を行

う。

【００５９】資源管理手段８０４は、資源０１に対するアクセス要求の認否を判定する手段である。入力手段０６からのアクセス要求の受信とそれによる起動、アクセス規則テーブル０８と属性保持装置１１の参照、識別子保持装置１０と属性情報テーブル８１４の参照、アクセス主体の属性の認否の判定、属性によるアクセス要求の認否の判定、属性保持装置１１へのアクセス主体の是認済属性の出力、出力手段０７へのアクセス不許可の送信と起動の指令、資源アクセス手段０５へのアクセス要求の送信と起動の指令、を行う。

【００６０】資源アクセス手段０５は、資源０１にアクセスできる手段である。資源管理手段８０４からのアクセス要求の受信とそれによる起動、アクセス要求の実行、出力手段０７への実行結果の送信と起動の指令、を行う。

【００６１】入力手段０６は、アクセス主体と情報システムとの対話を行う手段である。アクセス主体からのアクセス要求などの入力の受信、情報システム内の他の手段への情報の送信と起動の指令、を行う。

【００６２】出力手段０７は、アクセス主体と情報システムとの対話を行う手段である。情報システム内の他の手段からの情報の受信とそれによる起動、アクセス主体に対する処理結果などの出力、を行う。

【００６３】アクセス規則テーブル０８は、資源管理手段８０４がアクセス権限の検査を行うために用いるテーブルであり、例えば図2に示したように、情報システム内の全ての資源に対して、その資源にアクセス可能な属性が設定してある。

【００６４】アクセス主体情報保持装置０９は、アクセス主体の情報を保持する装置である。識別子保持装置１０は、実体認証手段０２で実体認証されたアクセス主体の、公開鍵証明書に記載されたアクセス主体の一意な識別子（例えば、電子メールアドレス）を保持する装置である。属性保持装置１１は、資源管理手段８０４で是認済のアクセス主体の属性を保持する装置である。

【００６５】属性情報テーブル８１４は、アクセス主体の識別子単位に属性を格納しているテーブルである。

【００６６】ＣＡ公開鍵格納装置１２は、第三者証明機関であるＣＡの公開鍵を格納しておく装置である。公開鍵ＣＡ公開鍵格納装置１３は、実体認証手段０２でアクセス主体の公開鍵証明書のＣＡ署名の検証に用いるための、公開鍵ＣＡの公開鍵を格納しておく装置である。

【００６７】以下、図4を参照して、情報システムの動作を説明する。

【００６８】アクセス主体が情報システムに送信できるのは、実体認証要求、アクセス要求である。

【００６９】まず最初に、実体認証要求の処理を順に説明する。

【００７０】アクセス主体は、公開鍵証明書を入力手段０６に入力する。この入力された公開鍵証明書は実体認証手段０２に送信されて、認証の成否の判定に用いられる。

【００７１】図6は実体認証手段０２の動作の一例を示すフローチャートである。公開鍵証明書を入力手段０６から受信した（２０１）実体認証手段０２は、公開鍵ＣＡ公開鍵格納装置１３から公開鍵ＣＡの公開鍵を読み出し（２０２）、公開鍵証明書の公開鍵ＣＡの署名の検証を行う（２０３）。署名の検証に失敗すれば（２０４）、認証は失敗で、出力手段０７にＣＡ署名無効を送信して、起動を指令する（２０５）。署名の検証が成功すれば（２０４）、公開鍵証明書からアクセス主体の公開鍵を読み出し（２０６）、アクセス主体の秘密鍵で正当性を主張する非対称暗号系における認証方法により、アクセス主体の実体認証を行う（２０７）。認証が失敗した場合は（２０８）、出力手段０７に送信して、起動を指令する（２０９）。認証が成功した場合は（２０８、２１０）、公開鍵証明書のアクセス主体の識別子（図5の場合、電子メールアドレス）を抽出して（２１１）、識別子保持装置１０に出力する（２１２）。そして、出力手段０７に認証成功を送信して、起動を指令する（２１３）。

【００７２】次に、アクセス要求の処理を順に説明する。

【００７３】アクセス要求は、アクセス主体が認証済のときに行う。アクセス主体は、資源０１へのアクセス要求を入力手段０６に入力する。この入力されたアクセス要求は資源管理手段８０４に送信される。第1の実施の形態と同様に、アクセス要求を入力手段０６から受信した（９０１）資源管理手段８０４は、アクセス規則テーブル０８を参照して、資源０１のアクセスに必要な属性を抽出する（９０２）。さらに、属性保持装置１１を参照してアクセスに必要な属性が是認済かを確認する（９０３）。属性が是認済であれば、資源０１へのアクセスを認可して（９０４）、資源アクセス手段０５にアクセス要求を送信して、起動を指令する（９０５）。資源アクセス手段０５は、アクセス要求を資源０１に対して実行し、その結果は出力手段０７に送信されてアクセス主体に出力される。

【００７４】属性が是認済でなければ、資源管理手段８０４は、識別子保持装置１０を参照して、アクセス主体が認証済であるかを確認する（９０６）。認証済でなければ、出力手段０７に認証要求の処理が必要であることを送信して、起動を指令する（９０７）。認証済であれば、識別子保持装置１０からアクセス主体の識別子を読み出し（９０８）、属性情報テーブル８１４を参照して（９０９）、資源０１のアクセスに必要な属性をアクセス主体が持っているかを検証する（９１０）。アクセス主体が属性を持っていない場合は、資源０１へのアクセスを不許可にして、出力手段０７にアクセス不許可を送

信して、起動を指令する（９１１）。アクセス主体が属性を持っている場合は、その属性を是認して（９１２）、アクセス主体の属性を属性値保持装置１１に出力して（９１３）、さらに、資源０１へのアクセスを認可して（９０４）、資源アクセス手段０５にアクセス要求を送信して、起動を指令する（９０５）。

【００７５】上述のように構成された本発明の第2の実施の形態によれば、アクセス主体の属性によりアクセス規則の設定を行うため、アクセス規則の設定が単純に行える。それにより、資源のアクセス規則の設定者（例えばサービスの提供者）は、アクセス主体を知らない場合でもアクセスを許可することが可能となる。また、アクセス主体の実体認証に公開鍵証明書を用いるので、情報システム内でのユーザ登録などの管理は必要ではなくなり、公開鍵ＣＡの公開鍵の保管のみを行えばよい。さらに、ユーザ情報はアクセス主体の方で提示してくるので、ユーザ登録の検索などの処理も必要ではなくなる。

【００７６】図7は本発明の第3の実施の形態を示す情報システムのブロック図である。第3の実施の形態では、公開鍵証明書を用いることによりアクセス主体の実体認証を行い、属性証明書という新規な証明書に記載されたアクセス主体の属性を是認して、アクセス規則に基づき資源に対するアクセスを制御する。

【００７７】そこでまず、属性証明書について説明する。

【００７８】図8は、属性証明書を発行する属性証明書発行装置のブロック図である。属性ＣＡは、アクセス主体の識別子・属性について、それが正当であると判断できれば、属性証明書発行装置を用いて、識別子・属性を記載した文書（属性証明書の本文）に、自身の秘密鍵でデジタル署名を行い、属性証明書を発行する。

【００７９】以下、図8を用いて属性証明書発行装置の構成を説明する。

【００８０】属性証明書発行装置は、識別子と属性から属性証明書の本文を作成する本文作成装置２１と、属性証明書の本文にデジタル署名を行い属性証明書の署名文を作成する署名文作成装置２２と、本文と署名文から属性証明書を作成する証明書作成手段２３と、属性ＣＡの秘密鍵を格納する秘密鍵格納装置６０１と、属性証明書の本文を保持する本文保持装置６０２と、属性証明書の署名文を保持する署名文保持装置６０３とから構成される。

【００８１】以下、図8を用いて属性証明書発行装置の動作を説明する。

【００８２】まず、アクセス主体の識別子・属性を、本文作成手段２１に送信し、属性証明書の本文を作成して、本文保持装置６０２に保持する。次に、署名文作成手段２２は、秘密鍵格納装置６０１から属性ＣＡの秘密鍵を読み出し、秘密鍵を用いて、本文保持装置６０２に保持されている属性証明書の本文にデジタル署名を行い、属性証明書の署名文を作り、署名文保持装置６０３に保持する。最後に、証明書作成手段２３は、本文保持装置６０２に保持されている属性証明書の本文と、署名文保持装置６０３に保持されている属性証明書の署名文より、属性証明書を作成する。

【００８３】図9は属性証明書の例である。７０１が属性証明書の本文であり、７０２が属性証明書の署名文である。この例では、電子メールアドレスをアクセス主体の識別子として用いている。

【００８４】次に、第3の実施の形態の情報システムを、情報システムの構成、各構成要素の機能、情報システムの動作の順で説明する。

【００８５】先ず、図7を参照して、情報システムの構成を説明する。

【００８６】情報システムは、資源０１を備え、アクセス主体からのアクセス要求などを管理する。また、情報システムは、資源０１の他に、アクセス要求の管理のために、実体認証手段０２と、属性検証手段０３と、資源管理手段０４と、資源アクセス手段０５と、入力手段０６と、出力手段０７と、アクセス規則テーブル０８と、アクセス主体情報保持装置０９とを有する。

【００８７】さらに、アクセス主体情報保持装置０９には、識別子保持装置１０と属性保持装置１１とが備えられる。

【００８８】また他に、ＣＡ公開鍵格納装置１２も用いるが、これについては情報システム内の装置として構成してもよいし、ネットワークで接続された外部に存在してもよい。

【００８９】さらに、ＣＡ公開鍵格納装置１２には、公開鍵ＣＡ公開鍵格納装置１３と属性ＣＡ公開鍵格納装置１４とが備えられる。

【００９０】以下、図7を参照して、情報システムの各構成要素の機能を説明する。

【００９１】実体認証手段０２は、公開鍵証明書によりアクセス主体の実体認証を行うための手段である。公開鍵証明書には、例えば図5に示したように、アクセス主体の公開鍵、アクセス主体の識別子（例えば電子メールアドレス）、氏名、証明書を発行したＣＡのデジタル署名が記載されている。実体認証手段０２は、入力手段０６からの公開鍵証明書と認証情報の受信とそれによる起動、公開鍵ＣＡ公開鍵格納装置１３からの公開鍵の読み出し、公開鍵証明書の公開鍵ＣＡの署名の検証、アクセス主体の非対称暗号系における認証方法による実体認証、および、識別子保持装置１０への認証済アクセス主体の公開鍵証明書に記載の識別子の出力、出力手段０７への認証結果の送信と起動の指令、を行う。

【００９２】属性検証手段０３は、属性証明書を用いてアクセス主体の属性の認否の判定を行うための手段である。属性証明書には、例えば図9に示したように、アクセス主体の属性、アクセス主体の識別子（公開証明書と

同じもので、例えば電子メールアドレス）、証明書を発行したＣＡのデジタル署名が記載されている。属性検証手段０３は、入力手段０６からの属性証明書の受信とそれによる起動、識別子保持装置１０の参照、属性ＣＡ公開鍵格納装置１４からの公開鍵の読み出し、属性証明書の属性ＣＡの署名の検証、アクセス主体の属性の認否の判定、および、属性保持装置１１へのアクセス主体の是認属性の出力、出力手段０７への属性検証結果の送信と起動の指令、を行う。

【００９３】資源管理手段０４は、資源０１に対するアクセス要求の認否を判定する手段である。入力手段０６からのアクセス要求の受信とそれによる起動、アクセス規則テーブル０８と属性保持装置１１の参照、属性によるアクセス要求の認否の判定、出力手段０７へのアクセス不許可の送信と起動の指令、資源アクセス手段０５へのアクセス要求の送信と起動の指令、を行う。

【００９４】資源アクセス手段０５は、資源０１にアクセスできる手段である。資源管理手段０４からのアクセス要求の受信とそれによる起動、アクセス要求の実行、出力手段０７への実行結果の送信と起動の指令、を行う。

【００９５】入力手段０６は、アクセス主体と情報システムとの対話を行う手段である。アクセス主体からのアクセス要求などの入力の受信、情報システム内の他の手段への情報の送信と起動の指令、を行う。

【００９６】出力手段０７は、アクセス主体と情報システムとの対話を行う手段である。情報システム内の他の手段からの情報の受信とそれによる起動、アクセス主体に対する処理結果などの出力、を行う。

【００９７】アクセス規則テーブル０８は、資源管理手段０４がアクセス権限の検査を行うために用いるテーブルであり、例えば図2に示したように、情報システム内の全ての資源に対して、その資源にアクセス可能な属性が設定してある。

【００９８】アクセス主体情報保持装置０９は、アクセス主体の情報を保持する装置である。識別子保持装置１０は、実体認証手段０２で実体認証されたアクセス主体の、公開鍵証明書に記載されたアクセス主体の一意な識別子（例えば、電子メールアドレス）を保持する装置である。属性保持装置１１は、属性検証手段０３で是認済のアクセス主体の属性を保持する装置である。

【００９９】ＣＡ公開鍵格納装置１２は、第三者証明機関であるＣＡの公開鍵を格納しておく装置である。公開鍵ＣＡ公開鍵格納装置１３は、実体認証手段０２でアクセス主体の公開鍵証明書のＣＡ署名の検証に用いるための、公開鍵ＣＡの公開鍵を格納しておく装置である。属性ＣＡ公開鍵格納装置１４は、属性検証手段０３でアクセス主体の属性証明書のＣＡ署名の検証に用いるための、属性ＣＡの公開鍵を格納しておく装置である。

【０１００】以下、図7を参照して、情報システムの動作を説明する。

【０１０１】アクセス主体は情報システムに、実体認証要求、属性是認要求、アクセス要求を送信できる。

【０１０２】まず最初に、実体認証要求の処理を順に説明する。

【０１０３】アクセス主体は、公開鍵証明書を入力手段０６に入力する。この入力された公開鍵証明書は実体認証手段０２に送信されて、認証の成否の判定に用いられる。公開鍵証明書を入力手段０６から受信した実体認証手段０２は、第2の実施の形態と同様に、公開鍵ＣＡ公開鍵格納装置１３から公開鍵ＣＡの公開鍵を読み出し（２０２）、公開鍵証明書の公開鍵ＣＡの署名の検証を行う（２０３）。署名の検証に失敗すれば（２０４）、認証は失敗で、出力手段０７にＣＡ署名無効を送信して、起動を指令する（２０５）。署名の検証が成功すれば（２０４）、公開鍵証明書からアクセス主体の公開鍵を読み出し（２０６）、アクセス主体の秘密鍵で正当性を主張する非対称暗号系における認証方法により、アクセス主体の実体認証を行う（２０７）。認証が失敗した場合は（２０８）、出力手段０７に送信して、起動を指令する（２０９）。認証が成功した場合は（２０８、２１０）、公開鍵証明書のアクセス主体の識別子（図5の場合、電子メールアドレス）を抽出して（２１１）、識別子保持装置１０に出力する（２１２）。そして、出力手段０７に認証成功を送信して、起動を指令する（２１３）。

【０１０４】次に、属性是認要求の処理を順に説明する。

【０１０５】属性是認要求は、アクセス主体が認証済のときに行う。アクセス主体は、入力手段０６に属性証明書を入力する。この入力された属性証明書は属性検証手段０３に送信されて、属性の認否の検証に用いられる。

【０１０６】図１０は属性検証手段０３の動作の一例を示すフローチャートである。属性証明書を入力手段０６から受信した（３０１）属性検証手段０３は、属性証明書からアクセス主体の識別子を抽出する（３０２）。次に、識別子保持装置１０を参照して、アクセス主体が認証済であるかを確認する（３０３）。認証済でなければ、出力手段０７に認証要求の処理が必要であることを送信して、起動を指令する（３０４）。認証済であれば、識別子保持装置１０からアクセス主体の識別子を読み出し（３０５）、属性証明書のアクセス主体の識別子と一致するかを確認する（３０６）。一致しなければ、出力手段０７に識別子の不一致を送信して、起動を指令する（３０７）。一致すれば、属性証明書はアクセス主体のものであると判断でき、属性ＣＡ公開鍵格納装置１４から属性ＣＡの公開鍵を読み出し（３０８）、属性証明書の属性ＣＡの署名の検証を行う（３０９）。署名の検証に失敗すれば（３１０）、出力手段０７にＣＡ署名無効を送信して、起動を指令する（３１１）。署名の検

証に成功すれば（３１０）、属性は是認されて（３１２）、属性を属性保持装置１１に出力する（３１３）。そして、出力手段０７に属性是認を送信して、起動を指令する（３１４）。

【０１０７】次に、アクセス要求の処理を順に説明する。アクセス要求は、アクセス主体が属性是認済のときに行う。アクセス主体は、資源０１へのアクセス要求を入力手段０６に入力する。この入力されたアクセス要求は資源管理手段０４に送信される。

【０１０８】図１１は資源管理手段０４の動作の一例を示すフローチャートである。アクセス要求を入力手段０６から受信した（４０１）資源管理手段０４は、アクセス規則テーブル０８を参照して、資源０１のアクセスに必要な属性を抽出する（４０２）。さらに、属性保持装置１１を参照してアクセスに必要な属性が是認済かを確認する（４０３）。属性が是認済であれば、資源０１へのアクセスを認可して（４０４）、資源アクセス手段０５にアクセス要求を送信して、起動を指令する（４０５）。資源アクセス手段０５は、アクセス要求を資源０１に対して実行し、その結果は出力手段０７に送信されてアクセス主体に出力される。属性が是認済でなければ、出力手段０７に属性是認要求の処理が必要であることを送信して、起動を指令する（４０６）。

【０１０９】上述のように構成された本発明の第3の実施の形態によれば、アクセス主体の属性によりアクセス規則の設定を行うため、アクセス規則の設定が単純に行える。それにより、資源のアクセス規則の設定者（例えばサービスの提供者）は、アクセス主体を知らない場合でもアクセスを許可することが可能となる。また、アクセス主体の実体認証に公開鍵証明書を用いるので、情報システム内でのユーザ登録などの管理は必要ではなくなり、公開鍵ＣＡの公開鍵の保管のみを行えばよい。さらに、ユーザ情報はアクセス主体の方で提示してくるので、ユーザ登録の検索などの処理も必要ではなくなる。またさらに、属性証明書を用いるので、多種多様の属性をアクセス主体の方で提示することができて、情報システムでの属性是認も容易に行える。さらにそれぞれの属性ＣＡがアクセス主体の一部の情報の属性のみを管理すればよいので繁雑な作業にはならない。

【０１１０】図１２は本発明の第4の実施の形態を示す情報システムのブロック図である。第4の実施の形態では、公開鍵証明書を用いることによりアクセス主体の実体認証を行い、且つ、その公開鍵証明書に記載されたアクセス主体の属性を是認して、アクセス規則に基づいて資源に対するアクセスを制御する。また、属性証明書の属性にアクセス主体の公開鍵が記載されている場合は、属性証明書を用いることによりアクセス主体の実体認証を行い、且つ、その属性証明書に記載されたアクセス主体の属性を是認して、アクセス規則に基づいて資源に対するアクセスを制御することもできる。即ち、第4の実施の形態では、１つの証明書で実体認証と属性の是認とを行う。

【０１１１】第4の実施の形態では、図5に示した公開鍵証明書の内容に、更に、アクセス主体の属性を追加した、例えば図１３に例示するような公開鍵証明書を用いることができる。

【０１１２】また、第4の実施の形態では、図9に示した属性証明書の内容に、更に、アクセス主体の公開鍵を追加した、例えば図１４に例示するような属性証明書を用いることができる。なお、属性証明書の本文７０１に記載される識別子には、アクセス主体の公開鍵を用いることも出来る。この場合、匿名性のある属性証明書を作成することが出来る。このような属性証明書は、図8に示した属性証明書発行装置において、入力の識別子としてアクセス主体の公開鍵を与えることで作成することができる。

【０１１３】以下、図１２を参照して、第4の実施の形態を、情報システムの構成、各構成要素の機能、情報システムの動作の順で説明する。

【０１１４】まず、情報システムの構成を説明する。

【０１１５】情報システムは、資源０１を備え、アクセス主体からのアクセス要求などを管理する。また、情報システムは、資源０１の他に、アクセス要求の管理のために、属性検証手段１１０３と、資源管理手段０４と、資源アクセス手段０５と、入力手段０６と、出力手段０７と、アクセス規則テーブル０８と、アクセス主体情報保持装置０９とを有する。

【０１１６】さらに、アクセス主体情報保持装置０９には、属性保持装置１１が備えられる。

【０１１７】また他に、ＣＡ公開鍵格納装置１２も用いるが、これについては情報システム内の装置として構成してもよいし、ネットワークで接続された外部に存在してもよい。

【０１１８】さらに、ＣＡ公開鍵格納装置１２には、公開鍵ＣＡ公開鍵格納装置１３と属性ＣＡ公開鍵格納装置１４とが備えられる。

【０１１９】以下、図１２を参照して、情報システムの各構成要素の機能を説明する。

【０１２０】属性検証手段１１０３は、公開鍵証明書または属性証明書を用いてアクセス主体の実体認証と属性検証とを行うための手段である。入力手段０６からの公開鍵証明書と認証情報の受信とそれによる起動、入力手段０６からの属性証明書と認証情報の受信とそれによる起動、公開鍵ＣＡ公開鍵格納装置１３からの公開鍵の読み出し、属性ＣＡ公開鍵格納装置１４からの公開鍵の読み出し、公開鍵証明書の公開鍵ＣＡの署名の検証、属性証明書の属性ＣＡの署名の検証、アクセス主体の非対称暗号系における認証方法による実体認証、および、属性保持装置１１へのアクセス主体の是認済属性の出力、出力手段０７への認証結果の送信と起動の指令、を行う。

【０１２１】資源管理手段０４は、資源０１に対するアクセス要求の認否を判定する手段である。入力手段０６からのアクセス要求の受信とそれによる起動、アクセス規則テーブル０８と属性保持装置１１の参照、属性によるアクセス要求の認否の判定、出力手段０７へのアクセス不許可の送信と起動の指令、資源アクセス手段０５へのアクセス要求の送信と起動の指令、を行う。

【０１２２】資源アクセス手段０５は、資源０１にアクセスできる手段である。資源管理手段０４からのアクセス要求の受信とそれによる起動、アクセス要求の実行、出力手段０７への実行結果の送信と起動の指令、を行う。

【０１２３】入力手段０６は、アクセス主体と情報システムとの対話を行う手段である。アクセス主体からのアクセス要求などの入力の受信、情報システム内の他の手段への情報の送信と起動の指令、を行う。

【０１２４】出力手段０７は、アクセス主体と情報システムとの対話を行う手段である。情報システム内の他の手段からの情報の受信とそれによる起動、アクセス主体に対する処理結果などの出力、を行う。

【０１２５】アクセス規則テーブル０８は、資源管理手段８０４がアクセス権限の検査を行うために用いるテーブルであり、例えば図2に示したように、情報システム内の全ての資源に対して、その資源にアクセス可能な属性が設定してある。

【０１２６】アクセス主体情報保持装置０９は、アクセス主体の情報を保持する装置である。属性保持装置１１は、属性検証手段１１０３で是認済のアクセス主体の属性を保持する装置である。第3の実施の形態と異なり、識別子保持装置１０は必要ない。

【０１２７】ＣＡ公開鍵格納装置１２は、第三者証明機関であるＣＡの公開鍵を格納しておく装置である。公開鍵ＣＡ公開鍵格納装置１３は、属性検証手段１１０３でアクセス主体の公開鍵証明書のＣＡ署名の検証に用いるための、公開鍵ＣＡの公開鍵を格納しておく装置である。属性ＣＡ公開鍵格納装置１４は、属性検証手段１１０３でアクセス主体の属性証明書のＣＡ署名の検証に用いるための、属性ＣＡの公開鍵を格納しておく装置である。

【０１２８】以下、図１２を参照して、情報システムの動作を説明する。

【０１２９】第4の実施の形態では、実体認証要求は送信しない。属性是認要求のときに、実体認証を行う。従って、アクセス主体は情報システムに、属性是認要求、アクセスが送信できる。

【０１３０】まず、属性是認要求の処理を順に説明する。

【０１３１】アクセス主体は、入力手段０６に公開鍵証明書または属性証明書を入力する。入力された公開鍵証明書または属性証明書は、属性検証手段１１０３に送信

されて、認証の成否の判定に用いられ、属性の認否の検証がされる。

【０１３２】図１５は属性検証手段１１０３の動作の一例を示すフローチャートである。属性証明書を入力手段０６から受信した（１２０１）属性検証手段１１０３は、属性ＣＡ公開鍵格納装置１４から属性ＣＡの公開鍵を読み出し（１２０２）、属性証明書の属性ＣＡの署名の検証を行う（１２０３）。署名の検証に失敗すれば（１２０４）、出力手段０７にＣＡ署名無効を送信して、起動を指令する（１２０５）。署名の検証が成功すれば（１２０４）、属性証明書からアクセス主体の公開鍵を読み出し（１２０６）、アクセス主体の秘密鍵で正当性を主張する非対称暗号系における認証方法により、アクセス主体の実体認証を行う（１２０７）。認証が失敗した場合は（１２０８）、出力手段０７に送信して、起動を指令する（１２０９）。認証が成功した場合は（１２０８、１２１０）、属性証明書のアクセス主体の属性を抽出して（１２１１）、属性保持装置１１に出力する（１２１２）。そして、出力手段０７に属性是認を送信して、起動を指令する（１２１３）。また、１２０１で属性証明書でなく、公開鍵証明書を受信した場合も、属性ＣＡ公開鍵格納装置１４の代わりに、公開鍵ＣＡ公開鍵格納装置１３から公開鍵ＣＡの公開鍵を読み出すが、その他についての処理は同様である。

【０１３３】次に、アクセス要求の処理を順に説明する。アクセス要求は、アクセス主体が属性是認済のときに行う。アクセス主体は、資源０１へのアクセス要求を入力手段０６に入力する。この入力されたアクセス要求は資源管理手段０４に送信される。アクセス要求を入力手段０６から受信した資源管理手段０４は、第3の実施の形態と同様に、アクセス規則テーブル０８を参照して、資源０１のアクセスに必要な属性を抽出する（４０２）。さらに、属性保持装置１１を参照してアクセスに必要な属性が是認済かを確認する（４０３）。属性が是認済であれば、資源０１へのアクセスを認可して（４０４）、資源アクセス手段０５にアクセス要求を送信して、起動を指令する（４０５）。資源アクセス手段０５は、アクセス要求を資源０１に対して実行し、その結果は出力手段０７に送信されてアクセス主体に出力される。属性が是認済でなければ、出力手段０７に属性是認要求の処理が必要であることを送信して、起動を指令する（４０６）。

【０１３４】上述のように構成された本発明の第4の実施の形態によれば、アクセス主体の属性によりアクセス規則の設定を行うため、アクセス規則の設定が単純に行える。それにより、資源のアクセス規則の設定者（例えばサービスの提供者）は、アクセス主体を知らない場合でもアクセスを許可することが可能となる。また、アクセス主体の実体認証に属性証明書または公開鍵証明書を用いるので、情報システム内でのユーザ登録などの管理

は必要ではなくなり、公開鍵ＣＡの公開鍵の保管のみを行えばよい。さらに、ユーザ情報はアクセス主体の方で提示してくるので、ユーザ登録の検索などの処理も必要ではなくなる。またさらに、属性証明書または公開鍵証明書によって、多種多様の属性をアクセス主体の方で提示することができて、情報システムでの属性是認も容易に行える。さらにそれぞれの属性ＣＡがアクセス主体の一部の情報の属性のみを管理すればよいので繁雑な作業にはならない。また、１つの証明書でアクセス主体の実体認証と属性の是認とを行うことができる。

【０１３５】図１６は本発明を適用した情報システムのハードウェア構成例を示すブロック図である。この情報システムは、ＣＰＵやメモリ等を有するコンピュータ１６０１と、アクセス主体となるユーザが利用する利用者端末１６０２と、記録媒体１６０３とから構成される。記録媒体１６０３は、ＣＤ－ＲＯＭ、磁気ディスク装置、半導体メモリ等の機械読み取り可能な記録媒体であり、ここに記録されたアクセス制御用プログラムは、コンピュータ１６０１に読み取られ、コンピュータ１６０１の動作を制御し、コンピュータ１６０１上に前述した第1、第2、第3または第4の実施の形態における各構成要素を実現する。

【０１３６】即ち、第1の実施の形態にあっては、コンピュータ１６０１上に、実体認証手段８０２と、資源管理手段８０４と、資源アクセス手段０５と、入力手段０６と、出力手段０７と、アクセス規則テーブル０８と、アクセス主体情報保持装置０９と、必要に応じてパスワード情報格納装置８１３および属性情報テーブル８１４とを実現する。

【０１３７】また、第2の実施の形態にあっては、コンピュータ１６０１上に、実体認証手段０２と、資源管理手段８０４と、資源アクセス手段０５と、入力手段０６と、出力手段０７と、アクセス規則テーブル０８と、アクセス主体情報保持装置０９と、必要に応じてＣＡ公開鍵格納装置１２および属性情報テーブル８１４とを実現する。

【０１３８】さらに、第3の実施の形態にあっては、コンピュータ１６０１上に、実体認証手段０２と、属性検証手段０３と、資源管理手段０４と、資源アクセス手段０５と、入力手段０６と、出力手段０７と、アクセス規則テーブル０８と、アクセス主体情報保持装置０９と、必要に応じてＣＡ公開鍵格納装置１２とを実現する。

【０１３９】また更に、第4の実施の形態にあっては、コンピュータ１６０１上に、属性検証手段１１０３と、資源管理手段０４と、資源アクセス手段０５と、入力手段０６と、出力手段０７と、アクセス規則テーブル０８と、アクセス主体情報保持装置０９と、必要に応じてＣＡ公開鍵格納装置１２とを実現する。

【０１４０】

【発明の効果】本発明の効果としては、アクセス規則の設定が単純に行えることが挙げられる。これは、アクセス主体の属性により、アクセス規則の設定を行うためである。それにより、資源のアクセス規則の設定者（例えばサービスの提供者）は、アクセス主体を知らない場合でもアクセスを許可することができる。

【０１４１】また、アクセス主体の実体認証に公開鍵証明書を利用すれば、情報システム内でのユーザ登録などの管理は必要ではなくなり、公開鍵ＣＡの公開鍵の保管のみを行えばよい。さらに、ユーザ情報はアクセス主体の方で提示してくるので、ユーザ登録の検索などの処理も必要ではなくなる。

【０１４２】さらに、属性証明書を用いれば、多種多様の属性をアクセス主体の方で提示することができて、情報システムでの属性是認も容易に行える。さらにそれぞれの属性ＣＡがアクセス主体の一部の情報の属性のみを管理すればよいので繁雑な作業にはならない。

【０１４３】これにより、情報システムでは限定された登録ユーザのみではなく、不特定多数のアクセス主体にサービスを提供することが可能になる。

【図面の簡単な説明】

【図１】本発明の第1の実施の形態における情報システムの構成を示すブロック図である。

【図２】本発明の第1～第4の実施の形態におけるアクセス規則テーブル０８の例を示す図である。

【図３】本発明の第1、第2の実施の形態における資源管理手段８０４の動作を示すフローチャートである。

【図４】本発明の第2の実施の形態における情報システムの構成を示すブロック図である。

【図５】公開鍵証明書の例を示す図である。

【図６】本発明の第2、第3の実施の形態における実体認証手段０２の動作を示すフローチャートである。

【図７】本発明の第3の実施の形態における情報システムの構成を示すブロック図である。

【図８】本発明の第3、第4の実施の形態における属性証明書発行装置の構成を示すブロック図である。

【図９】本発明の第3の実施の形態における属性証明書の例を示す図である。

【図１０】本発明の第3の実施の形態における属性検証手段０３の動作を示すフローチャートである。

【図１１】本発明の第3、第4の実施の形態における資源管理手段０４の動作を示すフローチャートである。

【図１２】本発明の第4の実施の形態における情報システムの構成を示すブロック図である。

【図１３】アクセス主体の属性の記述を含む公開鍵証明書の例を示す図である。

【図１４】本発明の第4の実施の形態における属性証明書の例を示す図である。

【図１５】本発明の第4の実施の形態における属性検証手段１１０３の動作を示すフローチャートである。

【図１６】本発明を適用した情報システムのハードウェ

ア構成例を示すブロック図である。

【符号の説明】

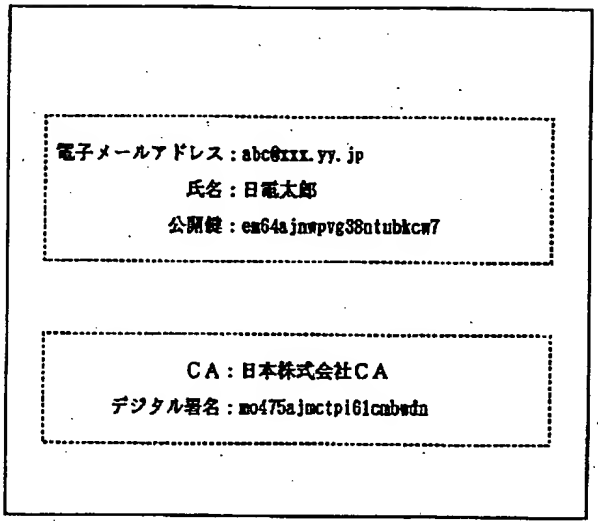
０１　資源
０２　実体認証手段
０３　属性検証手段
０４　資源管理手段
０５　資源アクセス手段
０６　入力手段
０７　出力手段
０８　アクセス規則テーブル
０９　アクセス主体情報保持装置
１０　識別子保持装置

１１　属性保持装置
１２　ＣＡ公開鍵格納装置
１３　公開鍵ＣＡ公開鍵格納装置
１４　属性ＣＡ公開鍵格納装置
２１　本文作成手段
２２　署名文作成手段
２３　証明書作成手段
８０２　実体認証手段
８０４　資源管理手段
８１３　パスワード情報格納装置
８１４　属性情報テーブル
１１０３　属性検証手段

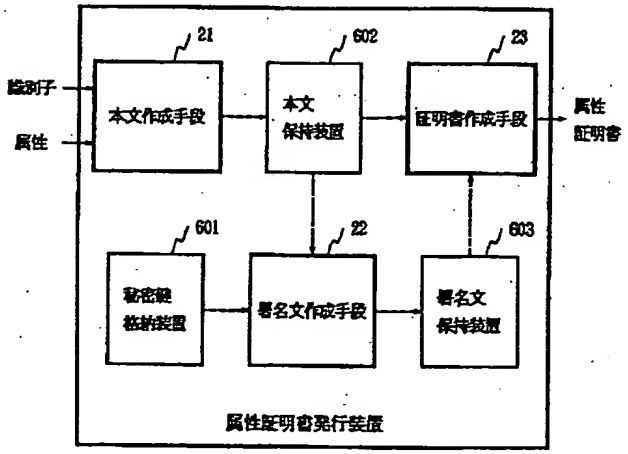
【図2】

属性＼資源	ファイルA	データベースB	サービスC
会社名：日本株式会社 && 部署名：X部 && 役職名：部長	書き込み可能		
免許：高等学校教諭専修		読み出し可能	
現在年月日－生年月日＞＝20年			実行可能

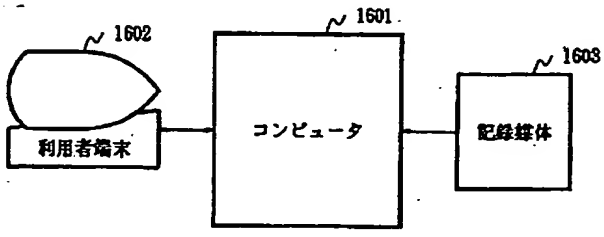
【図5】

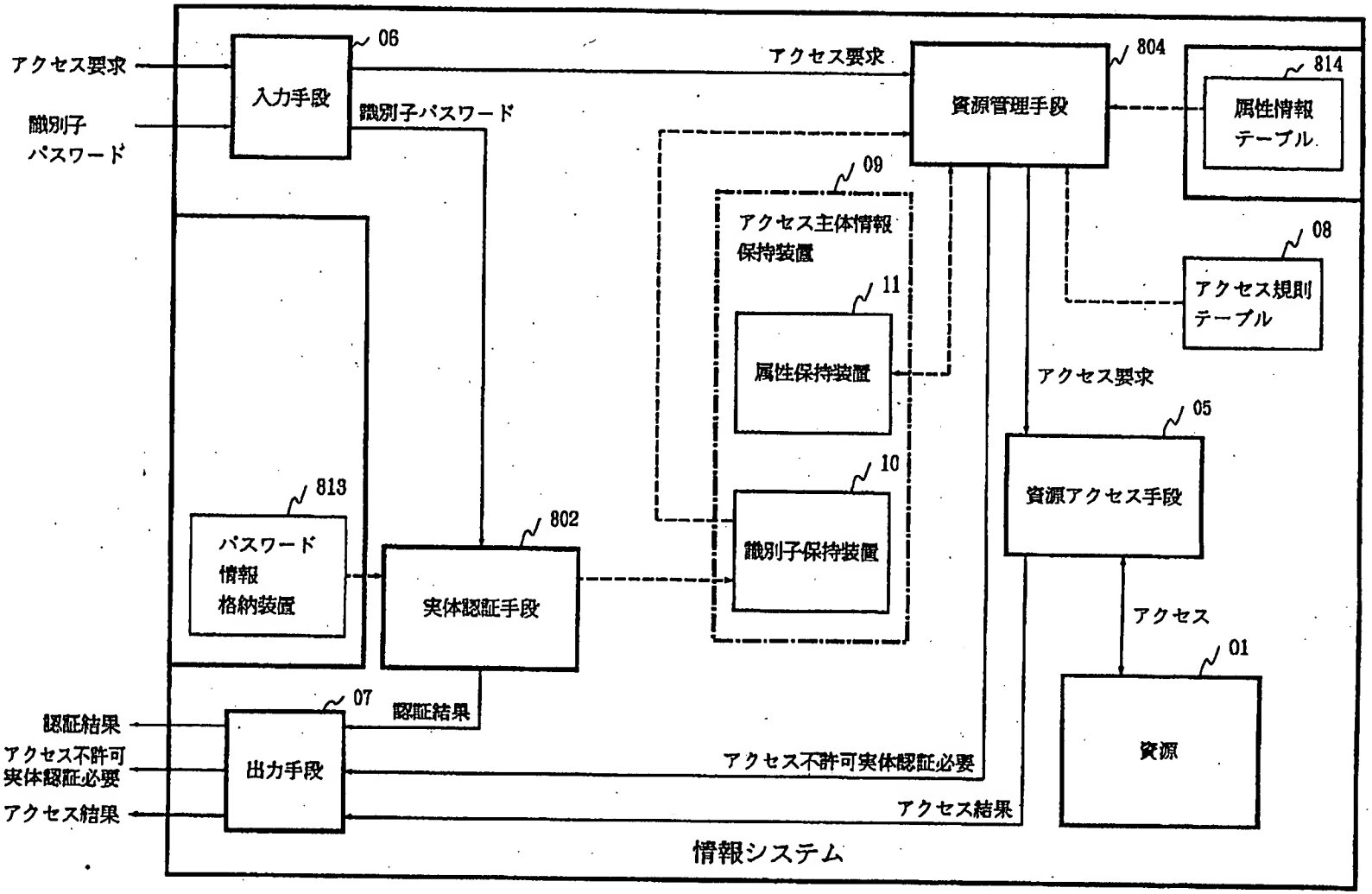


【図8】



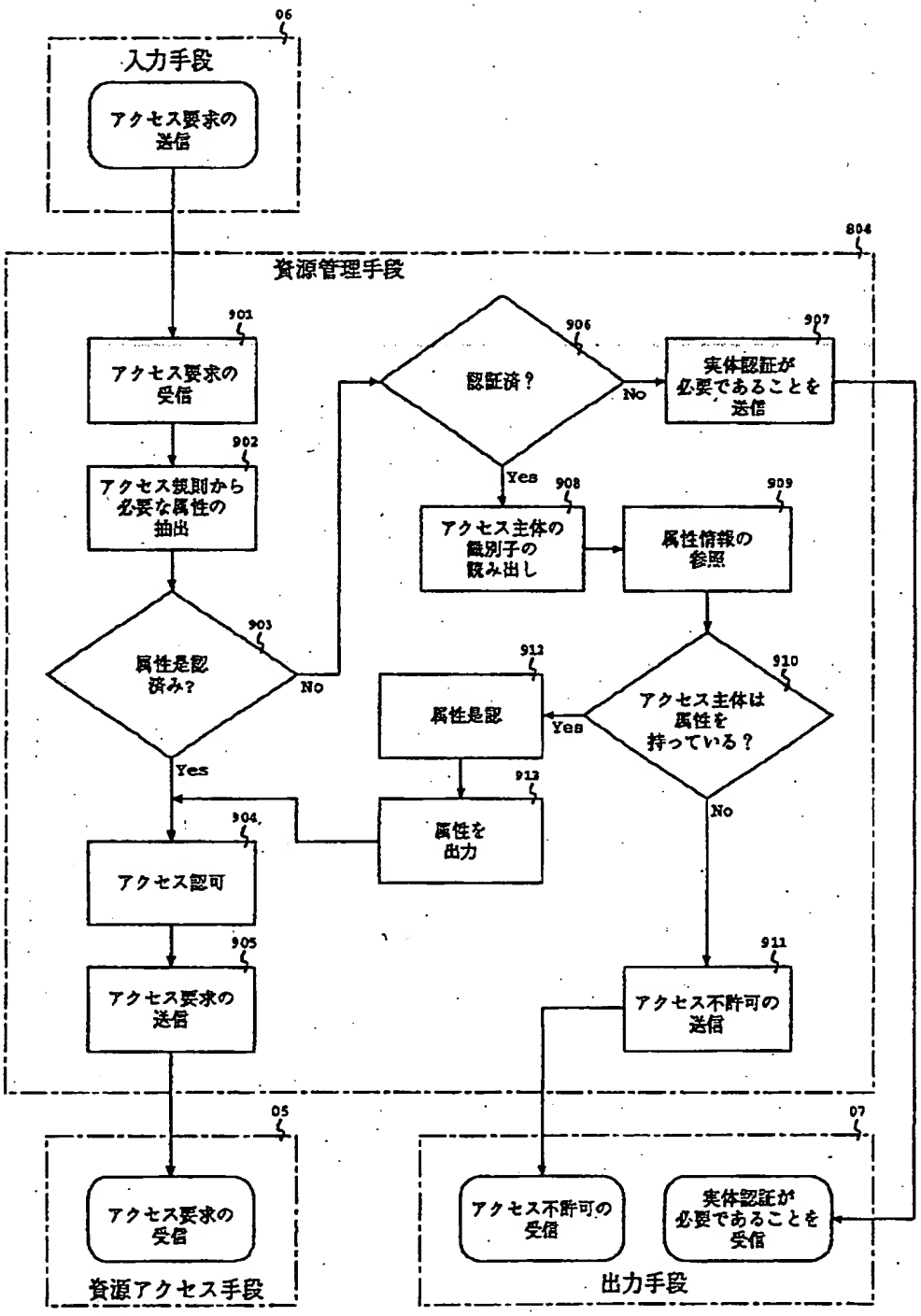
【図16】



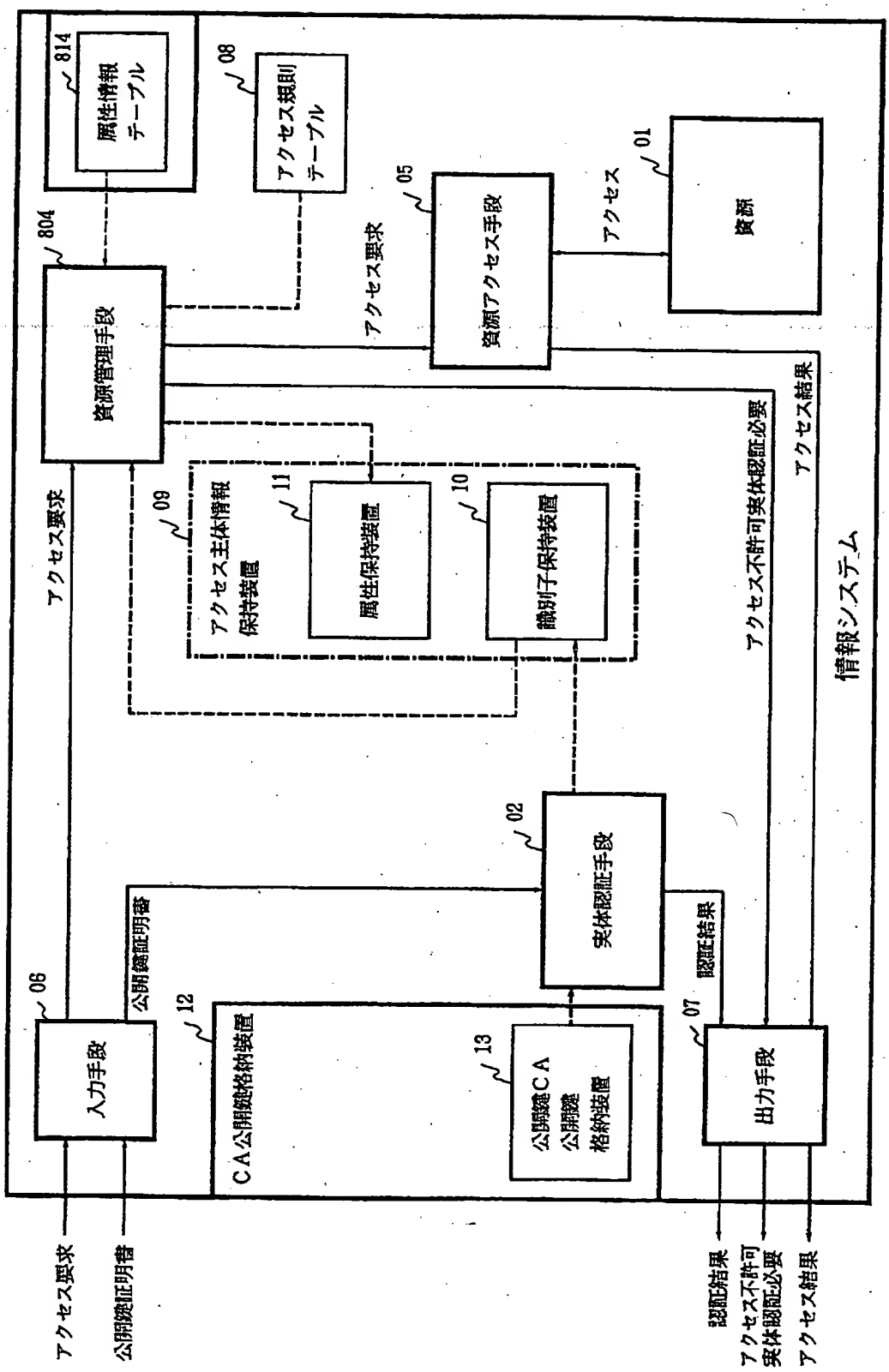

アクセス要求
識別子
パスワード
06
入力手段
識別子パスワード
アクセス要求
804
資源管理手段
814
属性情報
テーブル
09
アクセス主体情報
保持装置
11
属性保持装置
08
アクセス規則
テーブル
アクセス要求
05
資源アクセス手段
10
識別子保持装置
813
パスワード
情報
格納装置
802
実体認証手段
アクセス
01
資源
認証結果
07
認証結果
アクセス不許可
実体認証必要
出力手段
アクセス不許可実体認証必要
アクセス結果
アクセス結果
情報システム

【図1】

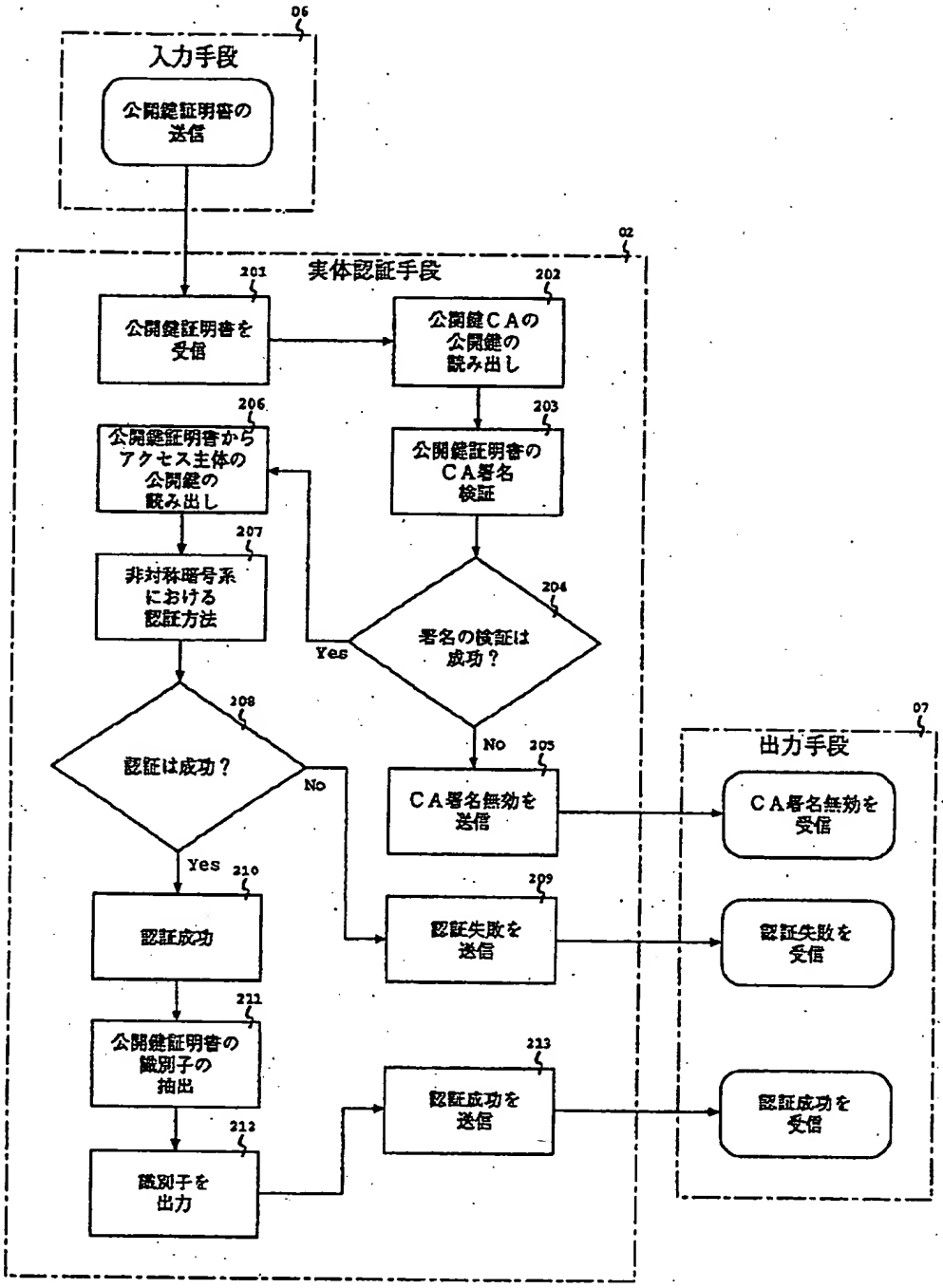
【図3】


06
入力手段
アクセス要求の送信
804
資源管理手段
901
アクセス要求の受信
902
アクセス規則から必要な属性の抽出
903
属性是認済み?
No
Yes
904
アクセス認可
905
アクセス要求の送信
906
認証済?
No
Yes
907
実体認証が必要であることを送信
908
アクセス主体の識別子の読み出し
909
属性情報の参照
910
アクセス主体は属性を持っている?
Yes
No
911
アクセス不許可の送信
912
属性是認
913
属性を出力
05
アクセス要求の受信
資源アクセス手段
07
アクセス不許可の受信
実体認証が必要であることを受信
出力手段

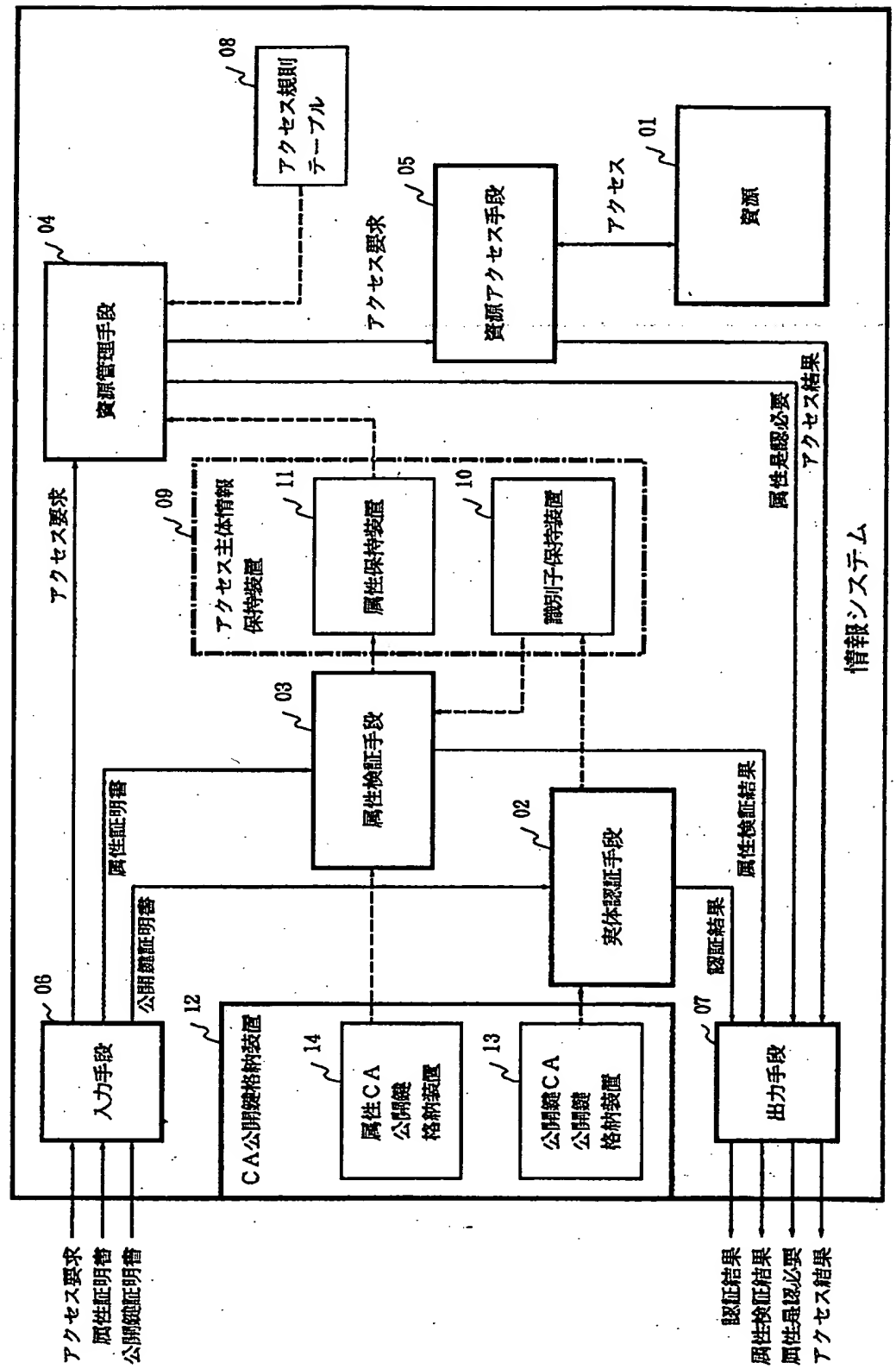
【図4】


情報システム
資源管理手段
804
属性情報テーブル
814
アクセス規則テーブル
08
アクセス要求
資源アクセス手段
05
アクセス
資源
01
アクセス主体情報保持装置
09
属性保持装置
11
識別子保持装置
10
アクセス要求
公開鍵証明書
入力手段
06
CA公開鍵格納装置
12
公開鍵CA公開鍵格納装置
13
実体認証手段
02
認証結果
出力手段
07
アクセス不許可実体認証必要
アクセス結果
アクセス要求
公開鍵証明書
認証結果
アクセス不許可実体認証必要
アクセス結果

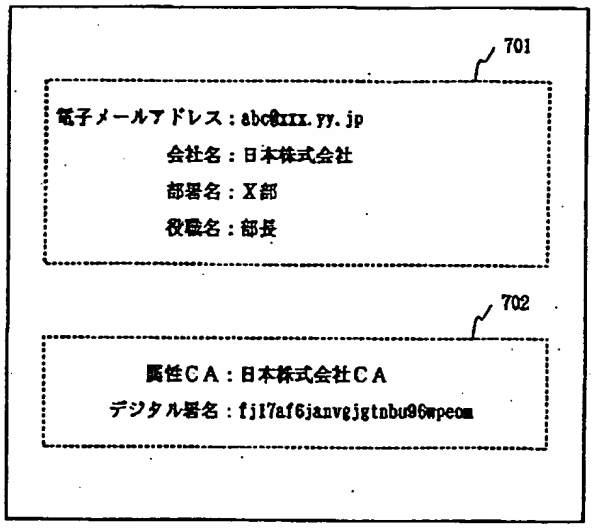
【 図6 】


06
入力手段
公開鍵証明書の送信
02
実体認証手段
201
公開鍵証明書を受信
202
公開鍵CAの公開鍵の読み出し
203
公開鍵証明書のCA署名検証
204
署名の検証は成功？
Yes
No
205
CA署名無効を送信
206
公開鍵証明書からアクセス主体の公開鍵の読み出し
207
非対称暗号系における認証方法
208
認証は成功？
No
Yes
209
認証失敗を送信
210
認証成功
211
公開鍵証明書の識別子の抽出
212
識別子を出力
213
認証成功を送信
07
出力手段
CA署名無効を受信
認証失敗を受信
認証成功を受信

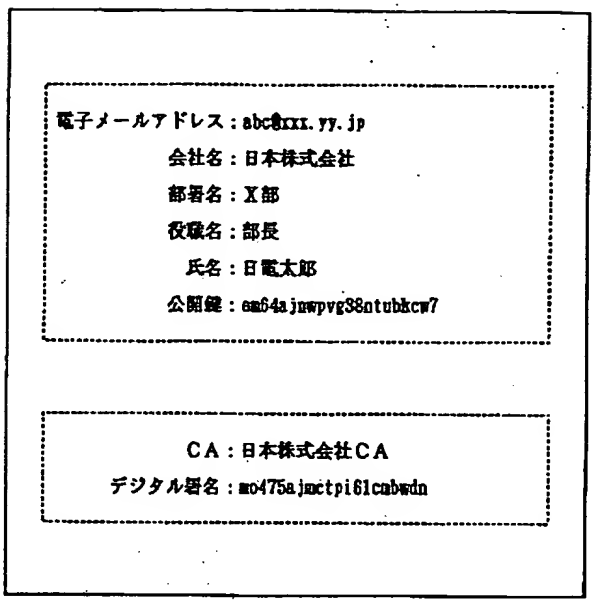
【図7】


情報システム
資源
01
資源アクセス手段
05
アクセス
アクセス規則テーブル
08
資源管理手段
04
アクセス要求
アクセス主体情報保持装置
09
属性保持装置
11
識別子保持装置
10
属性検証手段
03
実体認証手段
02
CA公開鍵格納装置
12
属性CA公開鍵格納装置
14
公開鍵CA公開鍵格納装置
13
入力手段
06
出力手段
07
属性証明書
公開鍵証明書
認証結果
属性検証結果
属性是認必要
アクセス結果
アクセス要求
属性証明書
公開鍵証明書
認証結果
属性検証結果
属性是認必要
アクセス結果

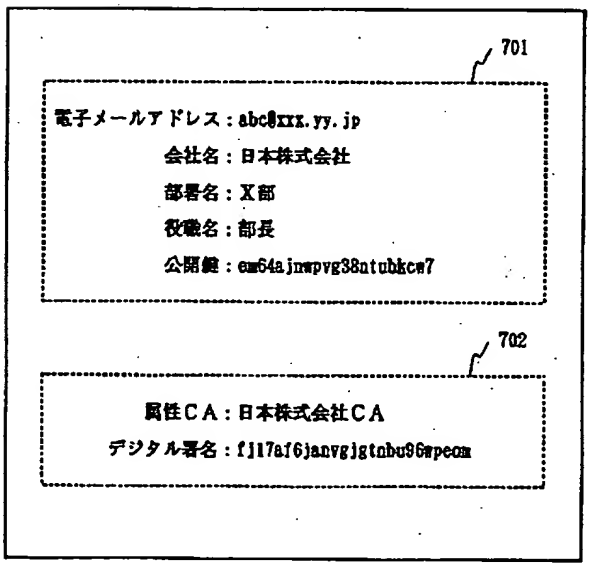
【図9】


701
電子メールアドレス：abc@xxx.yy.jp
会社名：日本株式会社
部署名：X部
役職名：部長
702
属性CA：日本株式会社CA
デジタル署名：fjl7af6janvgjgtnbu96wpeom

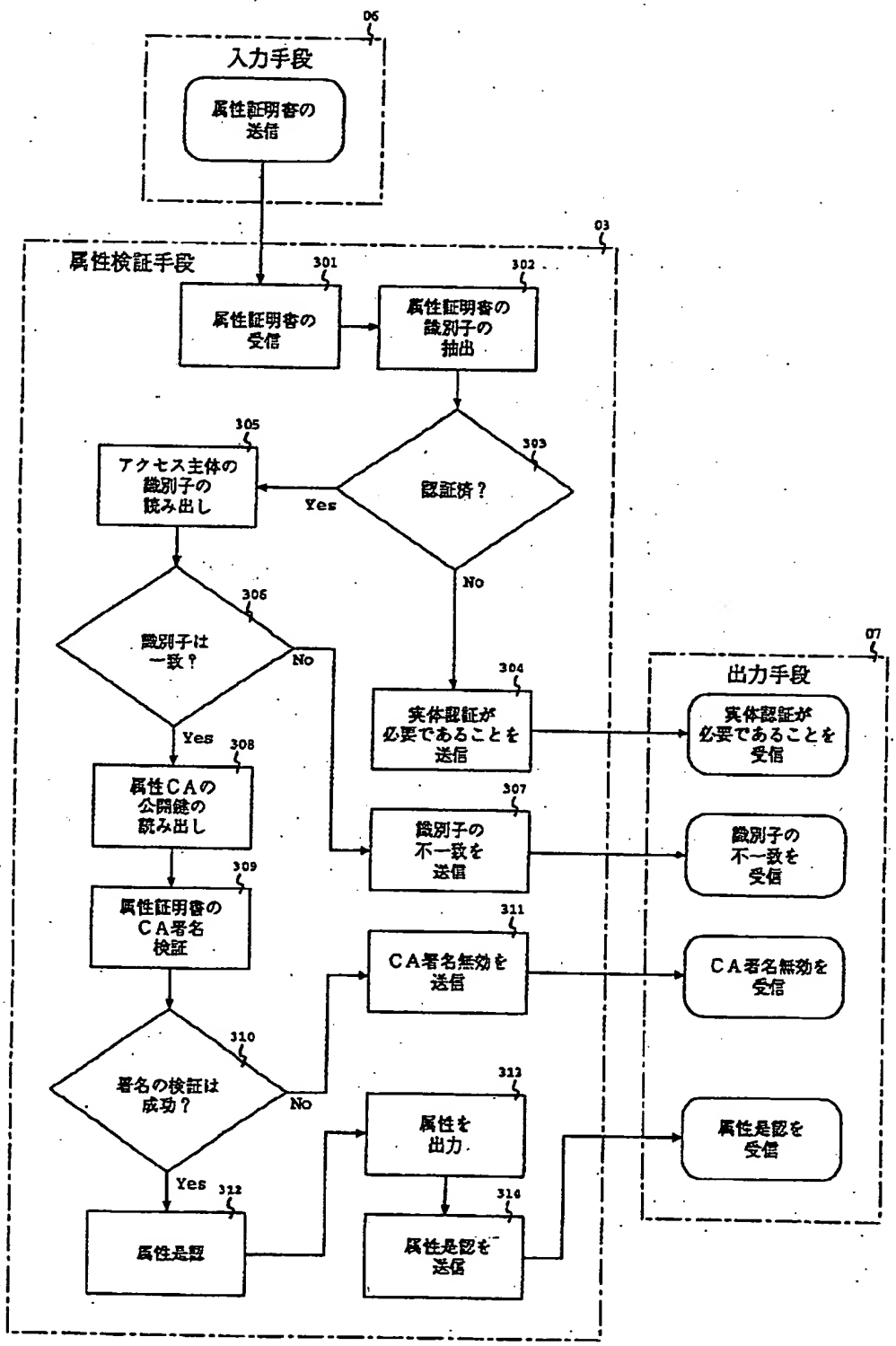
【図13】


電子メールアドレス：abc@xxx.yy.jp
会社名：日本株式会社
部署名：X部
役職名：部長
氏名：日電太郎
公開鍵：em64ajnwpvg38ntubkcw7
CA：日本株式会社CA
デジタル署名：mo475ajnctpi61cnbwdn

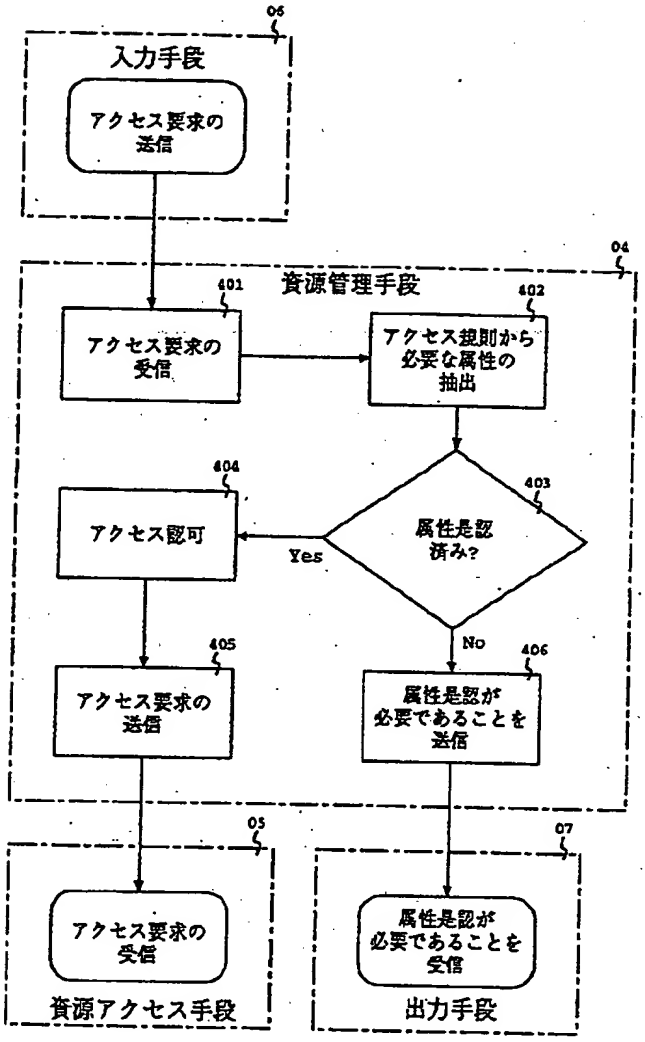
【図14】


701
電子メールアドレス：abc@xxx.yy.jp
会社名：日本株式会社
部署名：X部
役職名：部長
公開鍵：em64ajnwpvg38ntubkcw7
702
属性CA：日本株式会社CA
デジタル署名：fjl7af6janvgjgtnbu96wpeom

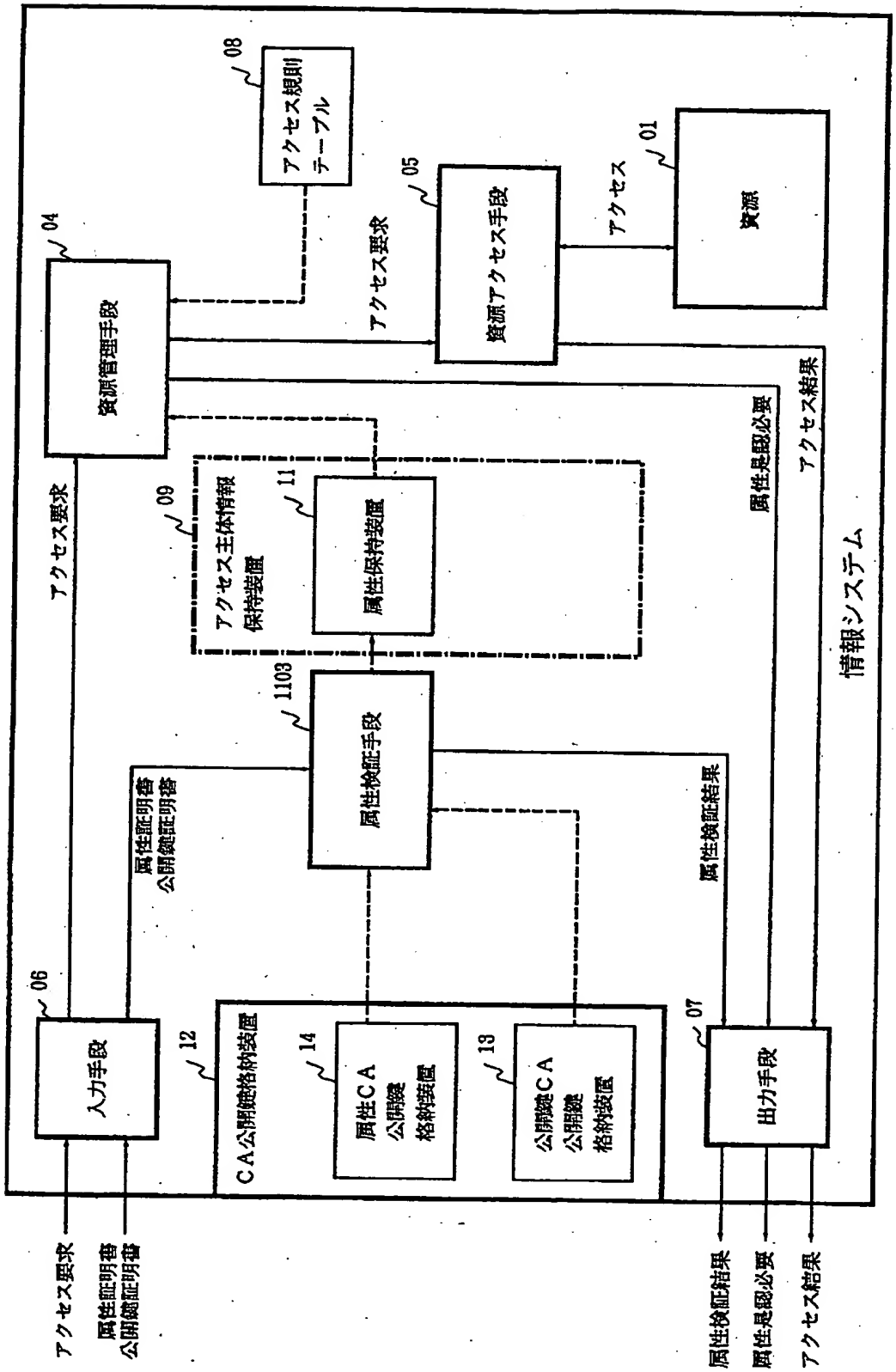
【図１０】


06
入力手段
属性証明書の送信
03
属性検証手段
301
属性証明書の受信
302
属性証明書の識別子の抽出
303
認証済？
Yes
305
アクセス主体の識別子の読み出し
No
306
識別子は一致？
No
Yes
308
属性CAの公開鍵の読み出し
309
属性証明書のCA署名検証
310
署名の検証は成功？
No
Yes
312
属性是認
304
実体認証が必要であることを送信
307
識別子の不一致を送信
311
CA署名無効を送信
313
属性を出力
314
属性是認を送信
07
出力手段
実体認証が必要であることを受信
識別子の不一致を受信
CA署名無効を受信
属性是認を受信

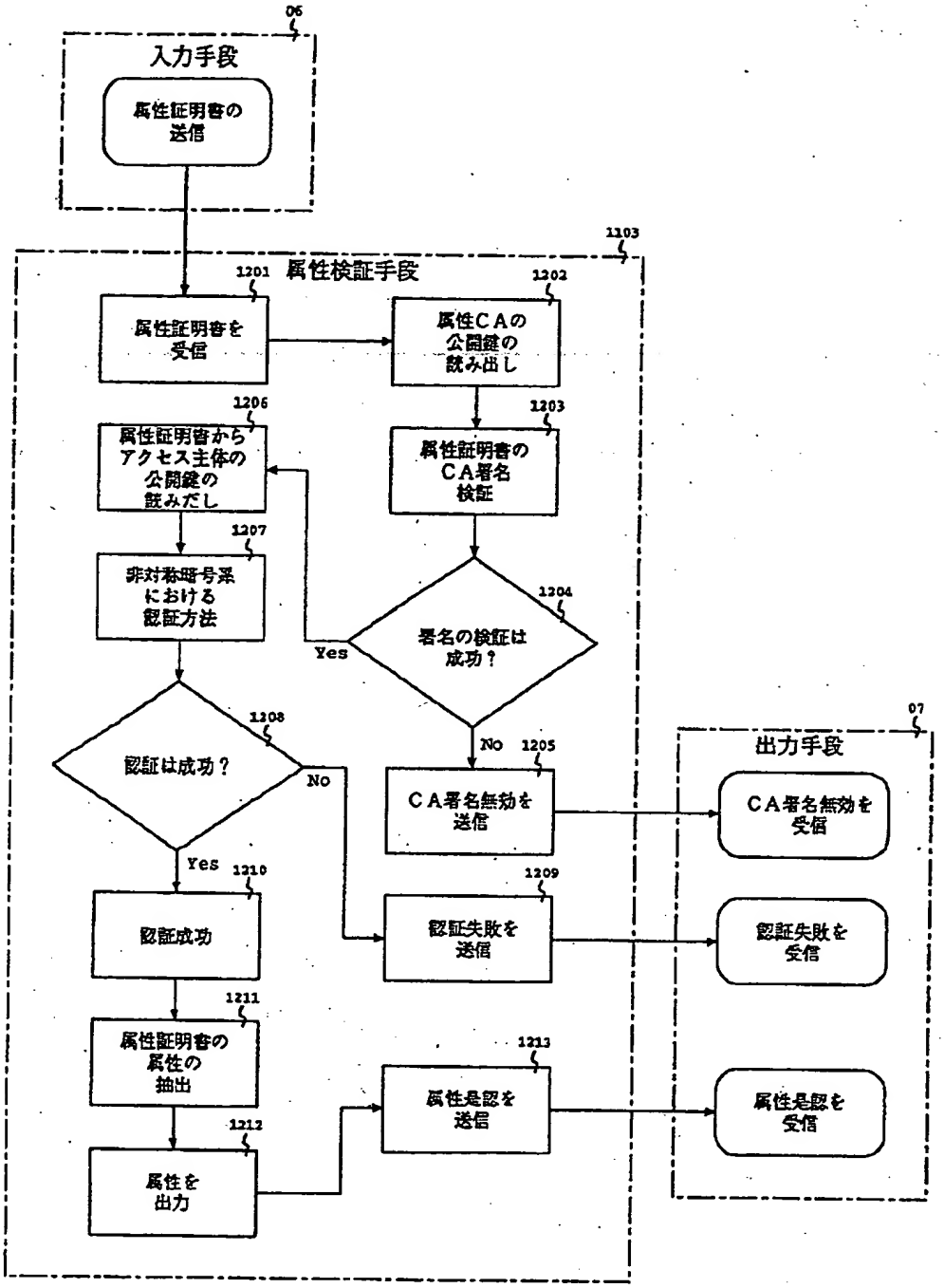
【図11】


06
入力手段
アクセス要求の送信
04
資源管理手段
401
アクセス要求の受信
402
アクセス規則から必要な属性の抽出
403
属性是認済み?
Yes
No
404
アクセス認可
405
アクセス要求の送信
406
属性是認が必要であることを送信
05
アクセス要求の受信
資源アクセス手段
07
属性是認が必要であることを受信
出力手段

【図12】


情報システム
資源管理手段
04
アクセス規則テーブル
08
資源アクセス手段
05
資源
01
アクセス
アクセス要求
アクセス結果
属性是認必要
アクセス主体情報保持装置
09
属性保持装置
11
属性検証手段
1103
属性証明書公開鍵証明書
属性検証結果
入力手段
06
CA公開鍵格納装置
12
属性CA公開鍵格納装置
14
公開鍵CA公開鍵格納装置
13
出力手段
07
アクセス要求
属性証明書公開鍵証明書
属性検証結果
属性是認必要
アクセス結果

【図１５】


06
入力手段
属性証明書の送信
1103
属性検証手段
1201
属性証明書を受信
1202
属性CAの公開鍵の読み出し
1206
属性証明書からアクセス主体の公開鍵の読みだし
1203
属性証明書のCA署名検証
1207
非対称暗号系における認証方法
1204
署名の検証は成功？
Yes
No
1208
認証は成功？
No
1205
CA署名無効を送信
07
出力手段
CA署名無効を受信
Yes
1210
認証成功
1209
認証失敗を送信
認証失敗を受信
1211
属性証明書の属性の抽出
1213
属性是認を送信
属性是認を受信
1212
属性を出力